OpenDJ Man Pages

Version 4.8.1-SNAPSHOT

Abstract

Helper to allow the doc build tools to find the man pages.

Table of Contents

Directory Server Tools

Table of Contents

backup

backup — back up OpenDJ directory data

backup

```
backup
```

1 Description

This utility can be used to back up one or more Directory Server backends.

2 Options

The **backup** command takes the following options:

Command options:

`-a | --backUpAll`

Back up all backends in the server.

Default: false

`-A | --hash`

Generate a hash of the backup contents.

Default: false

`-B | --incrementalBaseID {backupID}`

Backup ID of the source archive for an incremental backup.

`-c | --compress`

Compress the backup contents.

Default: false

`-d | --backupDirectory {backupDir}`

Path to the target directory for the backup file(s).

`-i | --incremental`

Perform an incremental backup rather than a full backup.

Default: false

`-I | --backupID {backupID}`

Use the provided identifier for the backup.

`-n | --backendID {backendName}`

Backend ID for the backend to archive.

`--offline`

Indicates that the command must be run in offline mode.

Default: false

`-s | --signHash`

Sign the hash of the backup contents.

Default: false

`-y | --encrypt`

Encrypt the backup contents.

Default: false

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

1

An error occurred.

4 Examples

The following example backs up all user data while the server is online.

```
$ backup -p 4444 -D "cn=Directory Manager" -w password \
 -a -d /path/to/opendj/bak -t 0
Backup task 20110613143801866 scheduled to start ...
```

The following example schedules back up of all user data every night at 2 AM when the server is online, and notifies diradmin@example.com when finished, or on error.

```
$ backup -p 4444 -D "cn=Directory Manager" -w password -a \
 -d /path/to/opendj/bak --recurringTask "00 02 * * *" \
 --completionNotify diradmin@example.com --errorNotify diradmin@example.com
Recurring Backup task BackupTask-988d6adf-4d65-44bf-8546-6ea74a2480b0
scheduled successfully
```

The following example backs up all user data while the server is offline.

```
$ stop-ds
Stopping Server...
...

$ backup --backupAll --backupDirectory /path/to/opendj/bak
... msg=The backup process completed successfully

$ start-ds
... The Directory Server has started successfully
```

backendstat

backendstat — gather OpenDJ backend debugging information

backendstat

```
backendstat {subcommand} {options}
```

1 Description

This utility can be used to debug a backend.

2 Options

The **backendstat** command takes the following options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Subcommands

The **backendstat** command supports the following subcommands:

3.1 backendstat dump-index

Dump records from an index, decoding keys and values. Depending on index size, this subcommand can generate lots of output.

3.1.1 Options

The **backendstat dump-index** command takes the following options:

`-n | --backendID {backendName}`

The backend ID of the backend.

`-b | --baseDN {baseDN}`

The base DN within the backend.

`-i | --indexName {indexName}`

The name of the index.

`-q | --statsOnly`

Do not display backend data, just statistics.

Default: false

`-K | --maxKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-k | --minKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-X | --maxHexKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-x | --minHexKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-S | --maxDataSize {maxDataSize}`

Only show records whose data is no larger than the provided value.

Default: -1

`-s | --minDataSize {minDataSize}`

Only show records whose data is no smaller than the provided value.

Default: -1

`-p | --skipDecode`

Do not try to decode backend data to their appropriate types.

Default: false

3.2 backendstat dump-raw-db

Dump the raw records in hexadecimal format for a low-level database within the pluggable backend's storage engine. Depending on index size, this subcommand can generate lots of output.

3.2.1 Options

The **backendstat dump-raw-db** command takes the following options:

`-n | --backendID {backendName}`

The backend ID of the backend.

`-d | --dbName {databaseName}`

The raw database name.

`-q | --statsOnly`

Do not display backend data, just statistics.

Default: false

`-K | --maxKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-k | --minKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-X | --maxHexKeyValue {maxKeyValue}`

Only show records with keys that should be ordered before the provided value using the comparator for the database container.

`-x | --minHexKeyValue {minKeyValue}`

Only show records with keys that should be ordered after the provided value using the comparator for the database container.

`-S | --maxDataSize {maxDataSize}`

Only show records whose data is no larger than the provided value.

Default: -1

`-s | --minDataSize {minDataSize}`

Only show records whose data is no smaller than the provided value.

Default: -1

`-l | --singleLine`

Write hexadecimal data on a single line instead of pretty format.

Default: false

3.3 backendstat list-backends

List the pluggable backends.

3.4 backendstat list-base-dns

List the base DNs in a backend.

3.4.1 Options

The **backendstat list-base-dns** command takes the following options:

`-n | --backendID {backendName}`

The backend ID of the backend.

3.5 backendstat list-indexes

List the indexes associated with a pluggable backend. This subcommand may take a long time to complete depending on the size of the backend.

3.5.1 Options

The **backendstat list-indexes** command takes the following options:

`-n | --backendID {backendName}`

The backend ID of the backend.

`-b | --baseDN {baseDN}`

The base DN within the backend.

3.6 backendstat list-raw-dbs

List the low-level databases within a pluggable backend's storage engine. This subcommand may take a long time to complete depending on the size of the backend.

3.6.1 Options

The **backendstat list-raw-dbs** command takes the following options:

`-n | --backendID {backendName}`

The backend ID of the backend.

`-u | --useSIUnits`

Uses SI Units for printing sizes.

Default: false

3.7 backendstat show-index-status

Shows the status of indexes for a backend base DN. This subcommand can take a long time to complete, as it reads all indexes for all backends.

When you run the 'list-index-status' command, the result is a table, followed by a "Total", which is the total number of indexes, followed by a list of indexes with "Over index-entry-limit keys" to show the values for which the number of entries exceeded the index entry limit. The table has the following columns.

Index Name

Name of the index, which takes the form *`attr.type`* for attribute indexes, and vlv.*`name`* for VLV indexes. Some indexes are for OpenDJ directory server's internal use.

Example: `givenName.caseIgnoreSubstringsMatch:6`

Tree Name

Name of the backend tree, which reflects how OpenDJ directory server organizes the data in the database.

Example: `/dc=example,dc=com/givenName.caseIgnoreSubstringsMatch:6`

Index Valid

This is `true` for valid indexes. If this is `false`, the index might be degraded. Verify the index, and rebuild the index if necessary.

Record Count

Number of indexed keys. Use the **backendstat dump-tree** command to see how many entry IDs correspond to each key.

Over Index Entry Limit

Number of keys for which there are too many values to maintain an index, based on the index entry limit. This is recorded as - for VLV indexes.

In other words, with the default index entry limit of 4000, if every user in your large directory has an email address ending in `@example.com`, and a substring index with default substring length of 6 is maintained for `mail`, then OpenDJ directory server does not maintain indexes for keys corresponding to substrings in `@example.com`.

As a result, an LDAP search with the filter `"(mail=*@example.com)"` becomes an unindexed search even though a substring index exists for the mail attribute. By default OpenDJ directory server does not allow unindexed searches except by privileged users. This is usually exactly the behavior you want in order to prevent client applications from sending searches that return every user in the directory for example. Clients should refine their search filters instead.

95%, 90%, 85%

Number of keys for which the number of values is approaching the index entry limit, having at least the specified percentage. This is a measure of how full the entry ID lists are.

3.7.1 Options

The **backendstat show-index-status** command takes the following options:

`-n | --backendID {backendName}`

The backend ID of the backend.

`-b | --baseDN {baseDN}`

The base DN within the backend.

4 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

5 Examples

The following example displays index information.

```
$ bin/backendstat dump-index  -n userRoot -b dc=example,dc=com -i id2childrencount

    Key (len 2): 1#52
    Value (len 8): 1
    Key (len 2): 2#52
    Value (len 8): 500000
    Key (len 9): Total Children Count
    Value (len 8): 500001

    Total Records: 3
    Total / Average Key Size: 13 bytes / 4 bytes
    Total / Average Data Size: 24 bytes / 8 bytes
```

base64

base64 — encode and decode base64 strings

base64

`base64` {subcommand} {options}

1 Description

This utility can be used to encode and decode information using base64.

2 Options

The **base64** command takes the following options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Subcommands

The **base64** command supports the following subcommands:

3.1 base64 decode

Decode base64-encoded information into raw data. When no options are specified, this subcommand reads from standard input and writes to standard output.

3.1.1 Options

The **base64 decode** command takes the following options:

`-d | --encodedData {data}`

The base64-encoded data to be decoded.

`-f | --encodedDataFile {path}`

The path to a file containing the base64-encoded data to be decoded.

`-o | --toRawFile {path}`

The path to a file to which the raw base64-decoded data should be written.

3.2 base64 encode

Encode raw data using base64. When no options are specified, this subcommand reads from standard input and writes to standard output.

3.2.1 Options

The **base64 encode** command takes the following options:

`-d | --rawData {data}`

The raw data to be base64 encoded.

`-f | --rawDataFile {path}`

The path to a file containing the raw data to be base64 encoded.

`-o | --toEncodedFile {path}`

The path to a file to which the base64-encoded data should be written.

4 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

5 Examples

The following command shows the changes from the external change log in human-readable format.

```
$ base64 decode -d YWRkOiBkZXNjcmlwdGlvbgpkZXNjcmlwdGlvbjogQSB0aGlyZCBjaGFuZ2UK\
LQpyZXBsYWNlOiBtb2RpZmllcnNOYW1lCm1vZGlmaWVyc05hbWU6IGNuPURpcmVjdG9yeSBNYW5hZ2V\
yLGNuPVJvb3QgRE5zLGNuPWNvbmZpZwotCnJlcGxhY2U6IG1vZGlmeVRpbWVzdGFtcAptb2RpZnlUaW\
1lc3RhbXA6IDIwMTEwNjEzMDcxMjEwWgotCg==
add: description
description: A third change
-
replace: modifiersName
modifiersName: cn=Directory Manager,cn=Root DNs,cn=config
-
replace: modifyTimestamp
modifyTimestamp: 20110613071210Z
-
```

control-panel

control-panel — start the OpenDJ graphical admin interface

control-panel

```
control-panel
```

1 Description

This utility can be used to display the Control Panel window which displays basic server information and allows to do some basic administration tasks on the server.

If no host name or port is provided, the tool will try to connect to the local server.

2 Options

The **control-panel** command takes the following options:

Command options:

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-r | --remote`

Connect to a remote server.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example starts the Control Panel on a remote host.

```
$ control-panel -r -h opendj.example.com -p 4444 &
```

create-rc-script

create-rc-script — script to manage OpenDJ as a service on UNIX

create-rc-script

```
create-rc-script
```

1 Description

Create an RC script that may be used to start, stop, and restart the Directory Server on UNIX-based systems.

2 Options

The **create-rc-script** command takes the following options:

Command options:

`-f | --outputFile {path}`

The path to the output file to create.

`-j | --javaHome {path}`

The path to the Java installation that should be used to run the server.

`-J | --javaArgs {args}`

A set of arguments that should be passed to the JVM when running the server.

`-u | --userName {userName}`

The name of the user account under which the server should run.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example adds a script to start OpenDJ at boot time on a Debian-based system, and then updates the runlevel system to use the script.

```
$ sudo create-rc-script -f /etc/init.d/opendj -u opendj-user
$ sudo update-rc.d opendj
```

dsconfig

dsconfig — manage OpenDJ directory server configuration

dsconfig

`dsconfig {subcommand} {options}`

1 Description

This utility can be used to define a base configuration for the Directory Server.

The **dsconfig** command is the primary command-line tool for viewing and editing OpenDJ configuration. When started without arguments, **dsconfig** prompts you for administration connection information, including the host name, administration port number, administrator bind DN and administrator password. The **dsconfig** command then connects securely to the directory server over the administration port. Once connected it presents you with a menu-driven interface to the server configuration.

When you pass connection information, subcommands, and additional options to **dsconfig**, the command runs in script mode and so is not interactive, though it can prompt you to ask whether to apply changes and whether to trust certificates (unless you use the `--no-prompt` and `--trustAll` options, respectively).

You can prepare **dsconfig** batch scripts by running the tool with the `--commandFilePath` option in interactive mode, then reading from the batch file with the `--batchFilePath` option in script mode. Batch files can be useful when you have many **dsconfig** commands to run and want to avoid starting the JVM for each command. Alternatively, you can read commands from standard input by using the `--batch` option.

The **dsconfig** command categorizes directory server configuration into *components*, also called *managed objects*. Actual components often inherit from a parent component type. For example, one component is a Connection Handler. An LDAP Connection Handler is a type of Connection Handler. You configure the LDAP Connection Handler component to specify how OpenDJ directory server handles LDAP connections coming from client applications.

Configuration components have *properties*. For example, the LDAP Connection Handler component has properties such as `listen-port` and `allow-start-tls`. You can set the component's `listen-port` property to `389` to use the default LDAP port number. You can set the component's `allow-start-tls` property to `true` to permit LDAP client applications to use StartTLS. Much of the configuration you do with **dsconfig** involves setting component properties.

2 Options

The **dsconfig** command takes the following options:

Command options:

`--batch`

Reads from standard input a set of commands to be executed.

Default: false

`--commandFilePath {path}`

The full path to the file where the equivalent non-interactive commands will be written when this command is run in interactive mode.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`--displayCommand`

Display the equivalent non-interactive argument in the standard output when this command is run in interactive mode.

Default: false

`--help-all`

Display all subcommands.

Default: false

`--help-core-server`

Display subcommands relating to core server.

Default: false

`--help-database`

Display subcommands relating to caching and back-ends.

Default: false

`--help-logging`

Display subcommands relating to logging.

Default: false

`--help-replication`

Display subcommands relating to replication.

Default: false

`--help-security`

Display subcommands relating to authentication and authorization.

Default: false

`--help-service-discovery`

Display subcommands relating to service discovery mechanism.

Default: false

`--help-user-management`

Display subcommands relating to user management.

Default: false

Configuration Options

`--advanced`

Allows the configuration of advanced components and properties.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-F | --batchFilePath {batchFilePath}`

Path to a batch file containing a set of commands to be executed.

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

`-s | --script-friendly`

Use script-friendly mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Subcommands

The **dsconfig** command provides many subcommands.

Subcommands let you create, list, and delete entire configuration components, and also let you get and set component properties. Subcommands therefore have names that reflect these five actions.

- create-*component*
- list-*component*s
- delete-*component*
- get-*component*-prop
- set-*component*-prop

Here, *component* names are names of managed object types. Subcommand *component* names are lower-case, hyphenated versions of the friendly names. When you act on an actual configuration component, you provide the name of the component as an option argument.

For example, the Log Publisher component has these corresponding subcommands.

- **create-log-publisher**

- **list-log-publishers**
- **delete-log-publisher**
- **get-log-publisher-prop**
- **set-log-publisher-prop**

When you create or delete Log Publisher components and when you get and set their configuration properties, you provide the name of the actual log publisher, which you can find by using the **list-log-publishers** subcommand.

```
$ dsconfig \
 list-log-publishers \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --trustAll

Log Publisher                 : Type                   : enabled
------------------------------:------------------------:--------
File-Based Access Logger      : file-based-access      : true
File-Based Audit Logger       : file-based-audit       : false
File-Based Debug Logger       : file-based-debug       : false
File-Based Error Logger       : file-based-error       : true
File-Based HTTP Access Logger : file-based-http-access : false
Replication Repair Logger     : file-based-error       : true

$ dsconfig \
 get-log-publisher-prop \
 --publisher-name "File-Based Access Logger" \
 --property rotation-policy \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --trustAll
Property        : Value(s)
----------------:-------------------------------------------------------------
rotation-policy : 24 Hours Time Limit Rotation Policy, Size Limit Rotation
                : Policy
```

Many subcommands let you set property values. Notice in the reference for the subcommands below that specific options are available for handling multi-valued properties. Whereas you can assign a single property value by using the `--set` option, you assign multiple values to a multi-valued property by using the `--add` option. You can reset the values of the multi-valued property by using the `--reset` option.

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot

necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Use the following options to view help for subcommands.

dsconfig --help-all

Display all subcommands

dsconfig --help-core-server

Display subcommands relating to core server

dsconfig --help-database

Display subcommands relating to caching and back-ends

dsconfig --help-logging

Display subcommands relating to logging

dsconfig --help-replication

Display subcommands relating to replication

dsconfig --help-security

Display subcommands relating to authentication and authorization

dsconfig --help-user-management

Display subcommands relating to user management

For help with individual subcommands, either use **dsconfig *`subcommand`* --help**, or start **dsconfig** in interactive mode, without specifying a subcommand.

To view all component properties, use the **dsconfig list-properties** command.

The **dsconfig** command supports the following subcommands:

- **dsconfig create-access-log-filtering-criteria**: Creates Access Log Filtering Criteria
- **dsconfig create-account-status-notification-handler**: Creates Account Status Notification Handlers
- **dsconfig create-alert-handler**: Creates Alert Handlers
- **dsconfig create-backend**: Creates Backends
- **dsconfig create-backend-index**: Creates Backend Indexes
- **dsconfig create-backend-vlv-index**: Creates Backend VLV Indexes
- **dsconfig create-certificate-mapper**: Creates Certificate Mappers
- **dsconfig create-connection-handler**: Creates Connection Handlers
- **dsconfig create-debug-target**: Creates Debug Targets
- **dsconfig create-entry-cache**: Creates Entry Caches
- **dsconfig create-extended-operation-handler**: Creates Extended Operation Handlers
- **dsconfig create-group-implementation**: Creates Group Implementations
- **dsconfig create-http-authorization-mechanism**: Creates HTTP Authorization Mechanisms
- **dsconfig create-http-endpoint**: Creates HTTP Endpoints
- **dsconfig create-identity-mapper**: Creates Identity Mappers
- **dsconfig create-key-manager-provider**: Creates Key Manager Providers
- **dsconfig create-log-publisher**: Creates Log Publishers
- **dsconfig create-log-retention-policy**: Creates Log Retention Policies
- **dsconfig create-log-rotation-policy**: Creates Log Rotation Policies
- **dsconfig create-monitor-provider**: Creates Monitor Providers
- **dsconfig create-password-generator**: Creates Password Generators
- **dsconfig create-password-policy**: Creates Authentication Policies
- **dsconfig create-password-storage-scheme**: Creates Password Storage Schemes
- **dsconfig create-password-validator**: Creates Password Validators

- **dsconfig create-plugin**: Creates Plugins
- **dsconfig create-replication-domain**: Creates Replication Domains
- **dsconfig create-replication-server**: Creates Replication Servers
- **dsconfig create-sasl-mechanism-handler**: Creates SASL Mechanism Handlers
- **dsconfig create-schema-provider**: Creates Schema Providers
- **dsconfig create-service-discovery-mechanism**: Creates Service Discovery Mechanisms
- **dsconfig create-synchronization-provider**: Creates Synchronization Providers
- **dsconfig create-trust-manager-provider**: Creates Trust Manager Providers
- **dsconfig create-virtual-attribute**: Creates Virtual Attributes
- **dsconfig delete-access-log-filtering-criteria**: Deletes Access Log Filtering Criteria
- **dsconfig delete-account-status-notification-handler**: Deletes Account Status Notification Handlers
- **dsconfig delete-alert-handler**: Deletes Alert Handlers
- **dsconfig delete-backend**: Deletes Backends
- **dsconfig delete-backend-index**: Deletes Backend Indexes
- **dsconfig delete-backend-vlv-index**: Deletes Backend VLV Indexes
- **dsconfig delete-certificate-mapper**: Deletes Certificate Mappers
- **dsconfig delete-connection-handler**: Deletes Connection Handlers
- **dsconfig delete-debug-target**: Deletes Debug Targets
- **dsconfig delete-entry-cache**: Deletes Entry Caches
- **dsconfig delete-extended-operation-handler**: Deletes Extended Operation Handlers
- **dsconfig delete-group-implementation**: Deletes Group Implementations
- **dsconfig delete-http-authorization-mechanism**: Deletes HTTP Authorization Mechanisms
- **dsconfig delete-http-endpoint**: Deletes HTTP Endpoints

- **dsconfig delete-identity-mapper**: Deletes Identity Mappers
- **dsconfig delete-key-manager-provider**: Deletes Key Manager Providers
- **dsconfig delete-log-publisher**: Deletes Log Publishers
- **dsconfig delete-log-retention-policy**: Deletes Log Retention Policies
- **dsconfig delete-log-rotation-policy**: Deletes Log Rotation Policies
- **dsconfig delete-monitor-provider**: Deletes Monitor Providers
- **dsconfig delete-password-generator**: Deletes Password Generators
- **dsconfig delete-password-policy**: Deletes Authentication Policies
- **dsconfig delete-password-storage-scheme**: Deletes Password Storage Schemes
- **dsconfig delete-password-validator**: Deletes Password Validators
- **dsconfig delete-plugin**: Deletes Plugins
- **dsconfig delete-replication-domain**: Deletes Replication Domains
- **dsconfig delete-replication-server**: Deletes Replication Servers
- **dsconfig delete-sasl-mechanism-handler**: Deletes SASL Mechanism Handlers
- **dsconfig delete-schema-provider**: Deletes Schema Providers
- **dsconfig delete-service-discovery-mechanism**: Deletes Service Discovery Mechanisms
- **dsconfig delete-synchronization-provider**: Deletes Synchronization Providers
- **dsconfig delete-trust-manager-provider**: Deletes Trust Manager Providers
- **dsconfig delete-virtual-attribute**: Deletes Virtual Attributes
- **dsconfig get-access-control-handler-prop**: Shows Access Control Handler properties
- **dsconfig get-access-log-filtering-criteria-prop**: Shows Access Log Filtering Criteria properties
- **dsconfig get-account-status-notification-handler-prop**: Shows Account Status Notification Handler properties
- **dsconfig get-administration-connector-prop**: Shows Administration Connector properties
- **dsconfig get-alert-handler-prop**: Shows Alert Handler properties

- **dsconfig get-backend-index-prop**: Shows Backend Index properties
- **dsconfig get-backend-prop**: Shows Backend properties
- **dsconfig get-backend-vlv-index-prop**: Shows Backend VLV Index properties
- **dsconfig get-certificate-mapper-prop**: Shows Certificate Mapper properties
- **dsconfig get-connection-handler-prop**: Shows Connection Handler properties
- **dsconfig get-crypto-manager-prop**: Shows Crypto Manager properties
- **dsconfig get-debug-target-prop**: Shows Debug Target properties
- **dsconfig get-entry-cache-prop**: Shows Entry Cache properties
- **dsconfig get-extended-operation-handler-prop**: Shows Extended Operation Handler properties
- **dsconfig get-external-changelog-domain-prop**: Shows External Changelog Domain properties
- **dsconfig get-global-configuration-prop**: Shows Global Configuration properties
- **dsconfig get-group-implementation-prop**: Shows Group Implementation properties
- **dsconfig get-http-authorization-mechanism-prop**: Shows HTTP Authorization Mechanism properties
- **dsconfig get-http-endpoint-prop**: Shows HTTP Endpoint properties
- **dsconfig get-identity-mapper-prop**: Shows Identity Mapper properties
- **dsconfig get-key-manager-provider-prop**: Shows Key Manager Provider properties
- **dsconfig get-log-publisher-prop**: Shows Log Publisher properties
- **dsconfig get-log-retention-policy-prop**: Shows Log Retention Policy properties
- **dsconfig get-log-rotation-policy-prop**: Shows Log Rotation Policy properties
- **dsconfig get-monitor-provider-prop**: Shows Monitor Provider properties
- **dsconfig get-password-generator-prop**: Shows Password Generator properties
- **dsconfig get-password-policy-prop**: Shows Authentication Policy properties
- **dsconfig get-password-storage-scheme-prop**: Shows Password Storage Scheme properties

- **dsconfig get-password-validator-prop**: Shows Password Validator properties
- **dsconfig get-plugin-prop**: Shows Plugin properties
- **dsconfig get-plugin-root-prop**: Shows Plugin Root properties
- **dsconfig get-replication-domain-prop**: Shows Replication Domain properties
- **dsconfig get-replication-server-prop**: Shows Replication Server properties
- **dsconfig get-root-dn-prop**: Shows Root DN properties
- **dsconfig get-root-dse-backend-prop**: Shows Root DSE Backend properties
- **dsconfig get-sasl-mechanism-handler-prop**: Shows SASL Mechanism Handler properties
- **dsconfig get-schema-provider-prop**: Shows Schema Provider properties
- **dsconfig get-service-discovery-mechanism-prop**: Shows Service Discovery Mechanism properties
- **dsconfig get-synchronization-provider-prop**: Shows Synchronization Provider properties
- **dsconfig get-trust-manager-provider-prop**: Shows Trust Manager Provider properties
- **dsconfig get-virtual-attribute-prop**: Shows Virtual Attribute properties
- **dsconfig get-work-queue-prop**: Shows Work Queue properties
- **dsconfig list-access-log-filtering-criteria**: Lists existing Access Log Filtering Criteria
- **dsconfig list-account-status-notification-handlers**: Lists existing Account Status Notification Handlers
- **dsconfig list-alert-handlers**: Lists existing Alert Handlers
- **dsconfig list-backend-indexes**: Lists existing Backend Indexes
- **dsconfig list-backend-vlv-indexes**: Lists existing Backend VLV Indexes
- **dsconfig list-backends**: Lists existing Backends
- **dsconfig list-certificate-mappers**: Lists existing Certificate Mappers
- **dsconfig list-connection-handlers**: Lists existing Connection Handlers
- **dsconfig list-debug-targets**: Lists existing Debug Targets

- **dsconfig list-entry-caches**: Lists existing Entry Caches
- **dsconfig list-extended-operation-handlers**: Lists existing Extended Operation Handlers
- **dsconfig list-group-implementations**: Lists existing Group Implementations
- **dsconfig list-http-authorization-mechanisms**: Lists existing HTTP Authorization Mechanisms
- **dsconfig list-http-endpoints**: Lists existing HTTP Endpoints
- **dsconfig list-identity-mappers**: Lists existing Identity Mappers
- **dsconfig list-key-manager-providers**: Lists existing Key Manager Providers
- **dsconfig list-log-publishers**: Lists existing Log Publishers
- **dsconfig list-log-retention-policies**: Lists existing Log Retention Policies
- **dsconfig list-log-rotation-policies**: Lists existing Log Rotation Policies
- **dsconfig list-monitor-providers**: Lists existing Monitor Providers
- **dsconfig list-password-generators**: Lists existing Password Generators
- **dsconfig list-password-policies**: Lists existing Password Policies
- **dsconfig list-password-storage-schemes**: Lists existing Password Storage Schemes
- **dsconfig list-password-validators**: Lists existing Password Validators
- **dsconfig list-plugins**: Lists existing Plugins
- **dsconfig list-properties**: Describes managed objects and their properties
- **dsconfig list-replication-domains**: Lists existing Replication Domains
- **dsconfig list-replication-server**: Lists existing Replication Server
- **dsconfig list-sasl-mechanism-handlers**: Lists existing SASL Mechanism Handlers
- **dsconfig list-schema-providers**: Lists existing Schema Providers
- **dsconfig list-service-discovery-mechanisms**: Lists existing Service Discovery Mechanisms
- **dsconfig list-synchronization-providers**: Lists existing Synchronization Providers

- **dsconfig list-trust-manager-providers**: Lists existing Trust Manager Providers
- **dsconfig list-virtual-attributes**: Lists existing Virtual Attributes
- **dsconfig set-access-control-handler-prop**: Modifies Access Control Handler properties
- **dsconfig set-access-log-filtering-criteria-prop**: Modifies Access Log Filtering Criteria properties
- **dsconfig set-account-status-notification-handler-prop**: Modifies Account Status Notification Handler properties
- **dsconfig set-administration-connector-prop**: Modifies Administration Connector properties
- **dsconfig set-alert-handler-prop**: Modifies Alert Handler properties
- **dsconfig set-backend-index-prop**: Modifies Backend Index properties
- **dsconfig set-backend-prop**: Modifies Backend properties
- **dsconfig set-backend-vlv-index-prop**: Modifies Backend VLV Index properties
- **dsconfig set-certificate-mapper-prop**: Modifies Certificate Mapper properties
- **dsconfig set-connection-handler-prop**: Modifies Connection Handler properties
- **dsconfig set-crypto-manager-prop**: Modifies Crypto Manager properties
- **dsconfig set-debug-target-prop**: Modifies Debug Target properties
- **dsconfig set-entry-cache-prop**: Modifies Entry Cache properties
- **dsconfig set-extended-operation-handler-prop**: Modifies Extended Operation Handler properties
- **dsconfig set-external-changelog-domain-prop**: Modifies External Changelog Domain properties
- **dsconfig set-global-configuration-prop**: Modifies Global Configuration properties
- **dsconfig set-group-implementation-prop**: Modifies Group Implementation properties
- **dsconfig set-http-authorization-mechanism-prop**: Modifies HTTP Authorization Mechanism properties
- **dsconfig set-http-endpoint-prop**: Modifies HTTP Endpoint properties

- **dsconfig set-identity-mapper-prop**: Modifies Identity Mapper properties
- **dsconfig set-key-manager-provider-prop**: Modifies Key Manager Provider properties
- **dsconfig set-log-publisher-prop**: Modifies Log Publisher properties
- **dsconfig set-log-retention-policy-prop**: Modifies Log Retention Policy properties
- **dsconfig set-log-rotation-policy-prop**: Modifies Log Rotation Policy properties
- **dsconfig set-monitor-provider-prop**: Modifies Monitor Provider properties
- **dsconfig set-password-generator-prop**: Modifies Password Generator properties
- **dsconfig set-password-policy-prop**: Modifies Authentication Policy properties
- **dsconfig set-password-storage-scheme-prop**: Modifies Password Storage Scheme properties
- **dsconfig set-password-validator-prop**: Modifies Password Validator properties
- **dsconfig set-plugin-prop**: Modifies Plugin properties
- **dsconfig set-plugin-root-prop**: Modifies Plugin Root properties
- **dsconfig set-replication-domain-prop**: Modifies Replication Domain properties
- **dsconfig set-replication-server-prop**: Modifies Replication Server properties
- **dsconfig set-root-dn-prop**: Modifies Root DN properties
- **dsconfig set-root-dse-backend-prop**: Modifies Root DSE Backend properties
- **dsconfig set-sasl-mechanism-handler-prop**: Modifies SASL Mechanism Handler properties
- **dsconfig set-schema-provider-prop**: Modifies Schema Provider properties
- **dsconfig set-service-discovery-mechanism-prop**: Modifies Service Discovery Mechanism properties
- **dsconfig set-synchronization-provider-prop**: Modifies Synchronization Provider properties
- **dsconfig set-trust-manager-provider-prop**: Modifies Trust Manager Provider properties
- **dsconfig set-virtual-attribute-prop**: Modifies Virtual Attribute properties
- **dsconfig set-work-queue-prop**: Modifies Work Queue properties

4 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

5 Examples

Much of the *OpenDJ Administration Guide* consists of **dsconfig** examples with text in between. This section therefore remains short.

The following example starts **dsconfig** in interactive, menu-driven mode on the default port of the current host.

```
$ dsconfig -h opendj.example.com -p 4444 -D "cn=Directory Manager" -w password

>>>> OpenDJ configuration console main menu

What do you want to configure?

    1)   Access Control Handler               22)  Log Publisher
    2)   Access Log Filtering Criteria        23)  Log Retention Policy
    3)   Account Status Notification Handler  24)  Log Rotation Policy
    4)   Administration Connector             25)  Monitor Provider
    5)   Alert Handler                        26)  Password Generator
    6)   Backend                              27)  Password Policy
    7)   Backend Index                        28)  Password Storage Scheme
    8)   Backend VLV Index                    29)  Password Validator
    9)   Certificate Mapper                   30)  Plugin
    10)  Connection Handler                   31)  Plugin Root
    11)  Crypto Manager                       32)  Replication Domain
    12)  Debug Target                         33)  Replication Server
    13)  Entry Cache                          34)  Root DN
    14)  Extended Operation Handler           35)  Root DSE Backend
    15)  External Changelog Domain            36)  SASL Mechanism Handler
    16)  Global Configuration                 37)  Schema Provider
    17)  Group Implementation                 38)  Synchronization Provider
    18)  HTTP Authorization Mechanism         39)  Trust Manager Provider
    19)  HTTP Endpoint                        40)  Virtual Attribute
    20)  Identity Mapper                      41)  Work Queue
    21)  Key Manager Provider

    q)   quit

Enter choice:
```

The following example demonstrates generating a batch file that corresponds to an interactive session enabling the debug log. The example then demonstrates using a modified batch file to disable the debug log.

```
$ dsconfig \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --commandFilePath ~/enable-debug-log.batch
 ...
$ cat ~/enable-debug-log.batch
# dsconfig session start date: 19/Oct/2011:08:52:22 +0000

# Session operation number: 1
# Operation date: 19/Oct/2011:08:55:06 +0000
dsconfig set-log-publisher-prop \
          --publisher-name File-Based\ Debug\ Logger \
          --set enabled:true \
          --hostname opendj.example.com \
          --port 4444 \
          --trustStorePath /path/to/opendj/config/admin-truststore \
          --bindDN cn=Directory\ Manager \
          --bindPassword ****** \
          --no-prompt

$ cp ~/enable-debug-log.batch ~/disable-debug-log.batch
$ vi ~/disable-debug-log.batch
$ cat ~/disable-debug-log.batch
set-log-publisher-prop \
          --publisher-name File-Based\ Debug\ Logger \
          --set enabled:false \
          --hostname opendj.example.com \
          --port 4444 \
          --trustStorePath /path/to/opendj/config/admin-truststore \
          --bindDN cn=Directory\ Manager \
          --bindPassword password \
          --no-prompt

$ dsconfig --batchFilePath ~/disable-debug-log.batch --no-prompt
set-log-publisher-prop
--publisher-name
File-Based Debug Logger
--set
enabled:false
--hostname
opendj.example.com
--port
4444
--trustStorePath
/path/to/opendj/config/admin-truststore
--bindDN
cn=Directory Manager
--bindPassword
password
--no-prompt

$
```

Notice that the original command file looks like a shell script with the bind password value replaced by asterisks. To pass the content as a batch file to **dsconfig**, strip `dsconfig` itself, and include the bind password for the

administrative user or replace that option with an alternative, such as reading the password from a file.

dsreplication

dsreplication — manage OpenDJ directory data replication

dsreplication

`dsreplication` {subcommand} {options}

1 Description

This utility can be used to configure replication between servers so that the data of the servers is synchronized. For replication to work you must first enable replication using the 'enable' subcommand and then initialize the contents of one of the servers with the contents of the other using the 'initialize' subcommand.

2 Options

The **dsreplication** command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN of the data to be replicated, initialized or for which we want to disable replication. Multiple base DNs can be provided by using this option multiple times.

`--commandFilePath {path}`

The full path to the file where the equivalent non-interactive commands will be written when this command is run in interactive mode.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`--displayCommand`

Display the equivalent non-interactive argument in the standard output when this command is run in interactive mode.

Default: false

`-j | --adminPasswordFile {bindPasswordFile}`

The file containing the password of the global administrator.

`-w | --adminPassword {bindPassword}`

The global administrator password.

Configuration Options

`--advanced`

Allows the configuration of advanced components and properties.

Default: false

LDAP connection options:

`-I | --adminUID {adminUID}`

User ID of the Global Administrator to use to bind to the server. For the 'enable' subcommand if no Global Administrator was defined previously for none of the server the Global Administrator will be created using the provided data.

Default: admin

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Subcommands

The **dsreplication** command supports the following subcommands:

3.1 dsreplication disable

Disables replication on the specified server for the provided base DN and removes references in the other servers with which it is replicating data.

3.1.1 Options

The **dsreplication disable** command takes the following options:

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-D | --bindDN {bindDN}`

DN to use to bind to the server where we want to disable replication. This option must be used when no Global Administrator has been defined on the server or if the user does not want to remove references in the other replicated servers. The password provided for the Global Administrator will be used when specifying this option.

Default: cn=Directory Manager

`-a | --disableReplicationServer`

Disable the replication server. The replication port and change log are disabled on the specified server.

Default: false

`--disableAll`

Disable the replication configuration on the specified server. The contents of the server are no longer replicated and the replication server (changelog and replication port) is disabled if it is configured.

Default: false

3.2 dsreplication enable

Updates the configuration of the servers to replicate the data under the specified base DN. If one of the specified servers is already replicating the data under the base DN with other servers, executing this subcommand will update the configuration of all the servers (so it is sufficient to execute the command line once for each server we add to the replication topology).

3.2.1 Options

The **dsreplication enable** command takes the following options:

`-h | --host1 {host}`

Fully qualified host name or IP address of the first server whose contents will be replicated.

Default: localhost.localdomain

`-p | --port1 {port}`

Directory server administration port number of the first server whose contents will be replicated.

Default: 4444

`-D | --bindDN1 {bindDN}`

DN to use to bind to the first server whose contents will be replicated. If not specified the global administrator will be used to bind.

Default: cn=Directory Manager

`--bindPassword1 {bindPassword}`

Password to use to bind to the first server whose contents will be replicated. If no bind DN was specified for the first server the password of the global administrator will be used to bind.

`--bindPasswordFile1 {bindPasswordFile}`

File containing the password to use to bind to the first server whose contents will be replicated. If no bind DN was specified for the first server the password of the global administrator will be used to bind.

`-r | --replicationPort1 {port}`

Port that will be used by the replication mechanism in the first server to communicate with the other servers. You have to specify this option only if replication was not previously configured in the first server.

Default: 8989

`--secureReplication1`

Specifies whether the communication through the replication port of the first server is encrypted or not. This option will only be taken into account the first time replication is configured on the first server.

Default: false

`--noReplicationServer1`

Do not configure a replication port or change log on the first server. The first server will contain replicated data but will not contain a change log of modifications made to the replicated data. Note that each replicated topology must contain at least two servers with a change log to avoid a single point of failure.

Default: false

`--onlyReplicationServer1`

Configure only a change log and replication port on the first server. The first server will not contain replicated data, but will contain a change log of the modifications made to the replicated data on other servers.

Default: false

`-O | --host2 {host}`

Fully qualified host name or IP address of the second server whose contents will be replicated.

Default: localhost.localdomain

`--port2 {port}`

Directory server administration port number of the second server whose contents will be replicated.

Default: 4444

`--bindDN2 {bindDN}`

DN to use to bind to the second server whose contents will be replicated. If not specified the global administrator will be used to bind.

Default: cn=Directory Manager

`--bindPassword2 {bindPassword}`

Password to use to bind to the second server whose contents will be replicated. If no bind DN was specified for the second server the password of the global administrator will be used to bind.

`-F | --bindPasswordFile2 {bindPasswordFile}`

File containing the password to use to bind to the second server whose contents will be replicated. If no bind DN was specified for the second server the password of the global administrator will be used to bind.

`-R | --replicationPort2 {port}`

Port that will be used by the replication mechanism in the second server to communicate with the other servers. You have to specify this option only if replication was not previously configured in the second server.

Default: 8989

`--secureReplication2`

Specifies whether the communication through the replication port of the second server is encrypted or not. This option will only be taken into account the first time replication is configured on the second server.

Default: false

`--noReplicationServer2`

Do not configure a replication port or change log on the second server. The second server will contain replicated data but will not contain a change log of modifications made to the replicated data. Note that each replicated topology must contain at least two servers with a change log to avoid a single point of failure.

Default: false

`--onlyReplicationServer2`

Configure only a change log and replication port on the second server. The second server will not contain replicated data, but will contain a change log of the modifications made to the replicated data on other servers.

Default: false

`-S | --skipPortCheck`

Skip the check to determine whether the specified replication ports are usable.

Default: false

`--noSchemaReplication`

Do not replicate the schema between the servers.

Default: false

`--useSecondServerAsSchemaSource`

Use the second server to initialize the schema of the first server. If this option nor option --noSchemaReplication are specified the schema of the first server will be used to initialize the schema of the second server.

Default: false

3.3 dsreplication initialize

Initialize the contents of the data under the specified base DN on the destination server with the contents on the source server. This operation is required after enabling replication in order replication to work ('initialize-all' can also be used for this purpose).

3.3.1 Options

The **dsreplication initialize** command takes the following options:

`-h | --hostSource {host}`

Fully qualified host name or IP address of the source server whose contents will be used to initialize the destination server.

Default: localhost.localdomain

`-p | --portSource {port}`

Directory server administration port number of the source server whose contents will be used to initialize the destination server.

Default: 4444

`-O | --hostDestination {host}`

Fully qualified host name or IP address of the destination server whose contents will be initialized.

Default: localhost.localdomain

`--portDestination {port}`

Directory server administration port number of the destination server whose contents will be initialized.

Default: 4444

3.4 dsreplication initialize-all

Initialize the contents of the data under the specified base DN on all the servers whose contents are being replicated with the contents on the specified server. This operation is required after enabling replication for replication to work ('initialize' applied to each server can also be used for this purpose).

3.4.1 Options

The **dsreplication initialize-all** command takes the following options:

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

3.5 dsreplication post-external-initialization

This subcommand must be called after initializing the contents of all the replicated servers using the tool import-ldif or the binary copy method. You must specify the list of base DNs that have been initialized and you must provide the credentials of any of the servers that are being replicated. See the usage of the subcommand 'pre-external-initialization' for more information.

3.5.1 Options

The **dsreplication post-external-initialization** command takes the following options:

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

3.6 dsreplication pre-external-initialization

This subcommand must be called before initializing the contents of all the replicated servers using the tool import-ldif or the binary copy method. You must specify the list of base DNs that will be initialized and you must provide the credentials of any of the servers that are being replicated. After calling this subcommand, initialize the contents of all the servers in the topology (use the same LDIF file/binary copy on each of the servers), then call the subcommand 'post-external-initialization'.

3.6.1 Options

The **dsreplication pre-external-initialization** command takes the following options:

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

3.7 dsreplication purge-historical

Launches a purge processing of the historical informations stored in the user entries by replication. Since this processing may take a while, you must specify the maximum duration for this processing.

3.7.1 Options

The **dsreplication purge-historical** command takes the following options:

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`--maximumDuration {maximum duration}`

This argument specifies the maximum duration the purge processing must last expressed in seconds.

Default: 3600

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

3.8 dsreplication reset-change-number

Re-synchronizes the change-log changenumber on one server with the change-log changenumber of another.

3.8.1 Options

The **dsreplication reset-change-number** command takes the following options:

`-h | --hostSource {host}`

Fully qualified host name or IP address of the source server whose contents will be used to initialize the destination server.

Default: localhost.localdomain

`-p | --portSource {port}`

Directory server administration port number of the source server whose contents will be used to initialize the destination server.

Default: 4444

`-O | --hostDestination {host}`

Fully qualified host name or IP address of the destination server whose contents will be initialized.

Default: localhost.localdomain

`--portDestination {port}`

Directory server administration port number of the destination server whose contents will be initialized.

Default: 4444

`--change-number {change number}`

The change number to use as the basis for re-synchronization.

3.9 dsreplication status

Displays a list with the basic replication configuration of the base DNs of the servers defined in the registration information. If no base DNs are specified as parameter the information for all base DNs is displayed.

3.9.1 Options

The **dsreplication status** command takes the following options:

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-s | --script-friendly`

Use script-friendly mode.

Default: false

4 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

5 Examples

The following example enables and then initializes replication for a new replica on `opendj2.example.com` from an existing replica on `opendj.example.com`.

```
$ dsreplication enable -I admin -w password -X -n -b dc=example,dc=com \
 --host1 opendj.example.com --port1 4444 --bindDN1 "cn=Directory Manager" \
 --bindPassword1 password --replicationPort1 8989 \
 --host2 opendj2.example.com --port2 4444 --bindDN2 "cn=Directory Manager" \
 --bindPassword2 password --replicationPort2 8989

Establishing connections ..... Done.
Checking registration information ..... Done.
Updating remote references on server opendj.example.com:4444 ..... Done.
Configuring Replication port on server opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
 opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
 opendj2.example.com:4444 ..... Done.
Updating registration configuration on server
 opendj.example.com:4444 ..... Done.
Updating registration configuration on server
 opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
 opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
 opendj2.example.com:4444 ..... Done.
Initializing registration information on server opendj2.example.com:4444 with
 the contents of server opendj.example.com:4444 ..... Done.
Initializing schema on server opendj2.example.com:4444 with the contents of
 server opendj.example.com:4444 ..... Done.

Replication has been successfully enabled.  Note that for replication to
 work you must initialize the contents of the base DN's that are being
  replicated (use dsreplication initialize to do so).

See
/var/.../opends-replication-7958637258600693490.log
for a detailed log of this operation.

$ dsreplication initialize-all -I admin -w password -X -n -b dc=example,dc=com \
 -h opendj.example.com -p 4444

Initializing base DN dc=example,dc=com with the contents from
 opendj.example.com:4444: 160 entries processed (100 % complete).
Base DN initialized successfully.

See
/var/.../opends-replication-5020375834904394170.log
for a detailed log of this operation.
```

encode-password

encode-password — encode a password with an OpenDJ storage scheme

encode-password

```
encode-password
```

1 Description

This utility can be used to encode user passwords with a specified storage scheme, or to determine whether a given clear-text value matches a provided encoded password.

2 Options

The **encode-password** command takes the following options:

Command options:

`-a | --authPasswordSyntax`

Use the authentication password syntax rather than the user password syntax.

Default: false

`-c | --clearPassword {clearPW}`

Clear-text password to encode or to compare against an encoded password.

`-e | --encodedPassword {encodedPW}`

Encoded password to compare against the clear-text password.

`-E | --encodedPasswordFile {file}`

Encoded password file.

`-f | --clearPasswordFile {file}`

Clear-text password file.

`-i | --interactivePassword`

The password to encode or to compare against an encoded password is interactively asked to the user.

Default: false

`-l | --listSchemes`

List available password storage schemes.

Default: false

`-r | --useCompareResultCode`

Use the LDAP compare result as an exit code for the password comparison.

Default: false

`-s | --storageScheme {scheme}`

Scheme to use for the encoded password.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

5

The `-r` option was used, and the compare did not match.

6

The `-r` option was used, and the compare did match.

other

An error occurred.

4 Examples

The following example encodes a password, and also shows comparison of a password with the encoded value.

```
$ encode-password -l
3DES
AES
BASE64
BCRYPT
BLOWFISH
CLEAR
CRYPT
MD5
PBKDF2
PKCS5S2
RC4
SHA
SMD5
SSHA
SSHA256
SSHA384
SSHA512

$ encode-password -c secret12 -s CRYPT
Encoded Password:  "{CRYPT}ZulJ6Dy3TFnrE"

$ encode-password -c secret12 -s CRYPT -e "{CRYPT}ZulJ6Dy3TFnrE" -r
The provided clear-text and encoded passwords match

$ echo $?
6
```

export-ldif

export-ldif — export OpenDJ directory data in LDIF

export-ldif

```
export-ldif
```

1 Description

This utility can be used to export data from a Directory Server backend in LDIF form.

2 Options

The **export-ldif** command takes the following options:

Command options:

`-a | --appendToLDIF`

Append an existing LDIF file rather than overwriting it.

Default: false

`-b | --includeBranch {branchDN}`

Base DN of a branch to include in the LDIF export.

`-B | --excludeBranch {branchDN}`

Base DN of a branch to exclude from the LDIF export.

`-c | --compress`

Compress the LDIF data as it is exported.

Default: false

`-e | --excludeAttribute {attribute}`

Attribute to exclude from the LDIF export.

`-E | --excludeFilter {filter}`

Filter to identify entries to exclude from the LDIF export.

`-i | --includeAttribute {attribute}`

Attribute to include in the LDIF export.

`-I | --includeFilter {filter}`

Filter to identify entries to include in the LDIF export.

`-l | --ldifFile {ldifFile}`

Path to the LDIF file to be written.

`-n | --backendID {backendName}`

Backend ID for the backend to export.

`-O | --excludeOperational`

Exclude operational attributes from the LDIF export.

Default: false

`--offline`

Indicates that the command must be run in offline mode.

Default: false

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`--wrapColumn {wrapColumn}`

Column at which to wrap long lines (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example exports data to a file, `Example.ldif`, with the server offline.

```
$ export-ldif -b dc=example,dc=com -n userRoot -l ../ldif/Example.ldif
... category=BACKEND severity=INFORMATION ...
...Exported 160 entries and skipped 0 in 0 seconds (average rate 1428.6/sec)
```

import-ldif

import-ldif — import OpenDJ directory data from LDIF

import-ldif

```
import-ldif
```

1 Description

This utility can be used to import LDIF data into a Directory Server backend, overwriting existing data. It cannot be used to append data to the backend database.

2 Options

The **import-ldif** command takes the following options:

Command options:

`-A | --templateFile {templateFile}`

Path to a MakeLDIF template to use to generate the import data.

`-b | --includeBranch {branchDN}`

Base DN of a branch to include in the LDIF import.

`-B | --excludeBranch {branchDN}`

Base DN of a branch to exclude from the LDIF import.

`-c | --isCompressed`

LDIF file is compressed.

Default: false

`--countRejects`

Count the number of entries rejected by the server and return that value as the exit code (values > 255 will be reduced to 255 due to exit code restrictions).

Default: false

`-e | --excludeAttribute {attribute}`

Attribute to exclude from the LDIF import.

`-E | --excludeFilter {filter}`

Filter to identify entries to exclude from the LDIF import.

`-F | --clearBackend`

Remove all entries for all base DNs in the backend before importing.

Default: false

`-i | --includeAttribute {attribute}`

Attribute to include in the LDIF import.

`-I | --includeFilter {filter}`

Filter to identify entries to include in the LDIF import.

`-l | --ldifFile {ldifFile}`

Path to the LDIF file to be imported.

`-n | --backendID {backendName}`

Backend ID for the backend to import.

`-O | --overwrite`

Overwrite an existing rejects and/or skip file rather than appending to it.

Default: false

`--offline`

Indicates that the command must be run in offline mode.

Default: false

`-R | --rejectFile {rejectFile}`

Write rejected entries to the specified file.

`-s | --randomSeed {seed}`

Seed for the MakeLDIF random number generator.

Default: 0

`-S | --skipSchemaValidation`

Skip schema validation during the LDIF import.

Default: false

`--skipFile {skipFile}`

Write skipped entries to the specified file.

`--threadCount {count}`

Number of threads used to read LDIF file during import. Default value (0) equals: 2 x (number of CPUs).

Default: 0

`--tmpdirectory {directory}`

Path to temporary directory for index scratch files during LDIF import.

Default: import-tmp

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode (no output).

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example imports the content of a file, `Example.ldif`, with the server offline.

```
$ import-ldif -b dc=example,dc=com -n userRoot -l /path/to/Example.ldif
... category=RUNTIME_INFORMATION severity=NOTICE...
... msg=Import LDIF environment close took 0 seconds
```

ldapcompare

ldapcompare — perform LDAP compare operations

ldapcompare

`ldapcompare` attribute:value DN

1 Description

This utility can be used to perform LDAP compare operations in the Directory Server.

2 Options

The **ldapcompare** command takes the following options:

Command options:

`--assertionFilter {filter}`

Use the LDAP assertion control with the provided filter.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *`controloid`* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`
`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`
`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`
`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`
`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`
`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`
`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`
`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`
`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-m | --useCompareResultCode`

Use the LDAP compare result as an exit code for the LDAP compare operations.

Default: false

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`-S | --scriptFriendly`

Use script-friendly mode.

Default: false

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

5

The LDAP compare operation did not match.

6

The `-m` option was used, and the LDAP compare operation did match.

ldap-error

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

4 Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

5 Examples

The following examples demonstrate comparing Babs Jensen's UID.

The following example uses a matching UID value.

```
$ ldapcompare -p 1389 uid:bjensen uid=bjensen,ou=people,dc=example,dc=com
Comparing type uid with value bjensen in entry
uid=bjensen,ou=people,dc=example,dc=com
Compare operation returned true for entry
uid=bjensen,ou=people,dc=example,dc=com
```

The following example uses a UID value that does not match.

```
$ ldapcompare -p 1389 uid:beavis uid=bjensen,ou=people,dc=example,dc=com
Comparing type uid with value beavis in entry
uid=bjensen,ou=people,dc=example,dc=com
Compare operation returned false for entry
uid=bjensen,ou=people,dc=example,dc=com
```

ldapdelete

ldapdelete — perform LDAP delete operations

ldapdelete

`ldapdelete` [DN]

1 Description

This utility can be used to perform LDAP delete operations in the Directory Server.

If standard input is used to specify entries to remove, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

2 Options

The **ldapdelete** command takes the following options:

Command options:

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *`controloid`* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

```
accountusable
accountusability
```

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`
`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`
`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`
`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`
`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`
`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`
`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`
`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`-x | --deleteSubtree`

Delete the specified entry and all entries below it.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

`ldap-error`

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

4 Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

5 Examples

The following command deletes a user entry from the directory.

```
$ ldapdelete -p 1389 -D "cn=Directory Manager" -w password \
 uid=bjensen,ou=people,dc=example,dc=com
Processing DELETE request for uid=bjensen,ou=people,dc=example,dc=com
DELETE operation successful for DN uid=bjensen,ou=people,dc=example,dc=com
```

The following command deletes the `ou=Groups` entry and all entries underneath `ou=Groups`.

```
$ ldapdelete -p 1389 -D "cn=Directory Manager" -w password -x \
 ou=groups,dc=example,dc=com
Processing DELETE request for ou=groups,dc=example,dc=com
DELETE operation successful for DN ou=groups,dc=example,dc=com
```

ldapmodify

ldapmodify — perform LDAP modify, add, delete, mod DN operations

ldapmodify

`ldapmodify` [changes_files ...]

1 Description

This utility can be used to perform LDAP modify, add, delete, and modify DN operations in the Directory Server. When not using file(s) to specify modifications, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

2 Options

The **ldapmodify** command takes the following options:

Command options:

`-a | --defaultAdd`

Legacy argument for ForgeRock OpenDJ compatibility.

Default: false

`--assertionFilter {filter}`

Use the LDAP assertion control with the provided filter.

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *`controloid`* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

```
accountusable
accountusability
```

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

```
authzid
authorizationidentity
```

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

```
effectiverights
geteffectiverights
```

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

```
managedsait
```

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

```
noop
no-op
```

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

```
pwpolicy
passwordpolicy
```

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

```
realattrsonly
realattributesonly
```

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

```
subtreedelete
treedelete
```

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

```
virtualattrsonly
virtualattributesonly
```

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`--postReadAttributes {attrList}`

Use the LDAP ReadEntry post-read control.

`--preReadAttributes {attrList}`

Use the LDAP ReadEntry pre-read control.

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

`ldap-error`

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

4 Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

5 Examples

The following example demonstrates use of the command to add an entry to the directory:

```
$ cat newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
facsimileTelephoneNumber: +1 408 555 1213
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
givenName: New
cn: New User
cn: Real Name
telephoneNumber: +1 408 555 1212
sn: Jensen
roomNumber: 1234
homeDirectory: /home/newuser
uidNumber: 10389
mail: newuser@example.com
l: South Pole
ou: Product Development
ou: People
gidNumber: 10636

$ ldapmodify -p 1389 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery newuser.ldif
Processing ADD request for uid=newuser,ou=People,dc=example,dc=com
ADD operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

The following listing shows a UNIX shell script that adds a user entry:

```
#!/bin/sh
#
# Add a new user with the ldapmodify utility.
#

usage(){
        echo "Usage: $0 uid firstname lastname"
        exit 1
}
[[ $# -lt 3 ]] && usage

LDAPMODIFY=/path/to/opendj/bin/ldapmodify
HOST=opendj.example.com
PORT=1389
ADMIN=uid=kvaughan,ou=people,dc=example,dc=com
PWD=bribery

$LDAPMODIFY -h $HOST -p $PORT -D $ADMIN -w $PWD <<EOF
dn: uid=$1,ou=people,dc=example,dc=com
uid: $1
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: $2 $3
givenName: $2
sn: $3
mail: $1@example.com
EOF
```

The following example demonstrates adding a Description attribute to the new user's entry:

```
$ cat newdesc.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
add: description
description: A new user's entry

$ ldapmodify -p 1389 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery newdesc.ldif
Processing MODIFY request for uid=newuser,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

The following example demonstrates changing the Description attribute for the new user's entry:

```
$ cat moddesc.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
replace: description
description: Another description

$ ldapmodify -p 1389 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery moddesc.ldif
Processing MODIFY request for uid=newuser,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

The following example demonstrates deleting the new user's entry:

```
$ cat deluser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: delete

$ ldapmodify -p 1389 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery deluser.ldif
Processing DELETE request for uid=newuser,ou=People,dc=example,dc=com
DELETE operation successful for DN uid=newuser,ou=People,dc=example,dc=com
```

ldappasswordmodify

ldappasswordmodify — perform LDAP password modifications

ldappasswordmodify

```
ldappasswordmodify
```

1 Description

This utility can be used to perform LDAP password modify operations in the Directory Server.

2 Options

The **ldappasswordmodify** command takes the following options:

Command options:

`-a | --authzID {authzID}`

Authorization ID for the user entry whose password should be changed. The authorization ID is a string having either the prefix "dn:" followed by the user's distinguished name, or the prefix "u:" followed by a user identifier that depends on the identity mapping used to match the user identifier to an entry in the directory. Examples include "dn:uid=bjensen,ou=People,dc=example,dc=com", and, if we assume that "bjensen" is mapped to Barbara Jensen's entry, "u:bjensen".

`-c | --currentPassword {currentPassword}`

Current password for the target user.

`-C | --currentPasswordFile {file}`

Path to a file containing the current password for the target user.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-F | --newPasswordFile {file}`

Path to a file containing the new password to provide for the target user.

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *`controloid`* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`
`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

`authzid`
`authorizationidentity`

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

`effectiverights`
`geteffectiverights`

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

`managedsait`

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

`noop`
`no-op`

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

`pwpolicy`
`passwordpolicy`

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

`realattrsonly`
`realattributesonly`

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

`subtreedelete`
`treedelete`

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

`virtualattrsonly`
`virtualattributesonly`

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

`-n | --newPassword {newPassword}`

New password to provide for the target user.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

`ldap-error`

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

4 Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

5 Examples

The following example demonstrates a user changing their own password.

```
$ cat /tmp/currpwd.txt /tmp/newpwd.txt
bribery
secret12

$ ldappasswordmodify -p 1389 -C /tmp/currpwd.txt --newPasswordFile /tmp/newpwd.txt \
 -D uid=kvaughan,ou=people,dc=example,dc=com -w bribery
The LDAP password modify operation was successful
```

ldapsearch

ldapsearch — perform LDAP search operations

ldapsearch

`ldapsearch` filter [attributes ...]

1 Description

This utility can be used to perform LDAP search operations in the Directory Server.

2 Options

The **ldapsearch** command takes the following options:

Command options:

`-a | --dereferencePolicy {dereferencePolicy}`

Alias dereference policy ('never', 'always', 'search', or 'find').

Default: never

`-A | --typesOnly`

Only retrieve attribute names but not their values.

Default: false

`--assertionFilter {filter}`

Use the LDAP assertion control with the provided filter.

`-b | --baseDN {baseDN}`

Search base DN.

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`-C | --persistentSearch ps[:changetype[:changesonly[:entrychgcontrols]]]`

Use the persistent search control.

A persistent search allows the client to continue receiving new results whenever changes are made to data that is in the scope of the search, thus using the search as a form of change notification.

The optional `changetype` setting defines the kinds of updates that result in notification. If you do not set the `changetype`, the default behavior is to send notifications for all updates.

`add`

Send notifications for LDAP add operations.

`del`
`delete`

Send notifications for LDAP delete operations.

`mod`
`modify`

Send notifications for LDAP modify operations.

`moddn`
`modrdn`
`modifydn`

Send notifications for LDAP modify DN (rename and move) operations.

`all`
`any`

Send notifications for all LDAP update operations.

The optional `changesonly` setting defines whether the server returns existing entries as well as changes.

`true`

Do not return existing entries, but instead only notifications about changes.

This is the default setting.

`false`

Also return existing entries.

The optional `entrychgcontrols` setting defines whether the server returns an Entry Change Notification control with each entry notification. The Entry Change Notification control provides additional information about the change

that caused the entry to be returned by the search. In particular, it indicates the change type, the change number if available, and the previous DN if the change type was a modify DN operation.

`true`

Do request the Entry Change Notification control.

This is the default setting.

`false`

Do not request the Entry Change Notification control.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`--countEntries`

Count the number of entries returned by the server.

Default: false

`-e | --getEffectiveRightsAttribute {attribute}`

Specifies geteffectiverights control specific attribute list.

`-g | --getEffectiveRightsAuthzid {authzID}`

Use geteffectiverights control with the provided authzid.

`-G | --virtualListView {before:after:index:count | before:after:value}`

Use the virtual list view control to retrieve the specified results page.

`-J | --control {controloid[:criticality[:value|::b64value|:<filePath]]}`

Use a request control with the provided information.

For some *`controloid`* values, you can replace object identifiers with user-friendly strings. The strings are listed here in lower case, but the case is not important. You can use camelCase if you prefer, for example.

`accountusable`
`accountusability`

Account Usability Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

```
authzid
authorizationidentity
```

Authorization Identity Request Control, Object Identifier: 2.16.840.1.113730.3.4.16

```
effectiverights
geteffectiverights
```

Get Effective Rights Request Control, Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

```
managedsait
```

Manage DSAIT Request Control, Object Identifier: 2.16.840.1.113730.3.4.2

```
noop
no-op
```

No-Op Control, Object Identifier: 1.3.6.1.4.1.4203.1.10.2

```
pwpolicy
passwordpolicy
```

Password Policy Control, Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

```
realattrsonly
realattributesonly
```

Real Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.17

```
subtreedelete
treedelete
```

Subtree Delete Request Control, Object Identifier: 1.2.840.113556.1.4.805

```
virtualattrsonly
virtualattributesonly
```

Virtual Attributes Only Request Control, Object Identifier: 2.16.840.1.113730.3.4.19

```
-l | --timeLimit {timeLimit}
```

Maximum length of time in seconds to allow for the search.

Default: 0

`--matchedValuesFilter {filter}`

Use the LDAP matched values control with the provided filter.

`-n | --dry-run`

Show what would be done but do not perform any operation.

Default: false

`-s | --searchScope {searchScope}`

Search scope ('base', 'one', 'sub', or 'subordinates'). Note: 'subordinates' is an LDAP extension that might not work with all LDAP servers.

Default: sub

`-S | --sortOrder {sortOrder}`

Sort the results using the provided sort order.

`--simplePageSize {numEntries}`

Use the simple paged results control with the given page size.

Default: 1000

`--subEntries`

Use subentries control to specify that subentries are visible and normal entries are not.

Default: false

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

`-z | --sizeLimit {sizeLimit}`

Maximum number of entries to return from the search.

Default: 0

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default:

`-E | --reportAuthzID`

Use the authorization identity control.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server port number.

Default: 389

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-q | --useStartTLS`

Use StartTLS to secure communication with the server.

Default: false

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`--usePasswordPolicyControl`

Use the password policy request control.

Default: false

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

`-Z | --useSSL`

Use SSL for secure communication with the server.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Filters

The filter argument is a string representation of an LDAP search filter as in `(cn=Babs Jensen)`, `(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))`, or `(cn:caseExactMatch:=Fred Flintstone)`.

4 Attributes

The optional attribute list specifies the attributes to return in the entries found by the search. In addition to identifying attributes by name such as `cn sn mail` and so forth, you can use the following notations, too.

*

Return all user attributes such as `cn`, `sn`, and `mail`.

+

Return all operational attributes such as `etag` and `pwdPolicySubentry`.

`@`*`objectclass`*

Return all attributes of the specified object class, where *`objectclass`* is one of the object classes on the entries returned by the search.

`1.1`

Return no attributes, only the DNs of matching entries.

5 Exit Codes

0

The command completed successfully.

`ldap-error`

An LDAP error occurred while processing the operation.

LDAP result codes are described in RFC 4511. Also see the additional information for details.

89

An error occurred while parsing the command-line arguments.

6 Files

You can use `~/.opendj/tools.properties` to set the defaults for bind DN, host name, and port number as in the following example.

```
hostname=directory.example.com
port=1389
bindDN=uid=kvaughan,ou=People,dc=example,dc=com

ldapcompare.port=1389
ldapdelete.port=1389
ldapmodify.port=1389
ldappasswordmodify.port=1389
ldapsearch.port=1389
```

7 Examples

The following example searches for entries with UID containing `jensen`, returning only DNs and uid values:

```
$ ldapsearch -p 1389 -b dc=example,dc=com "(uid=*jensen*)" uid
dn: uid=ajensen,ou=People,dc=example,dc=com
uid: ajensen

dn: uid=bjensen,ou=People,dc=example,dc=com
uid: bjensen

dn: uid=gjensen,ou=People,dc=example,dc=com
uid: gjensen

dn: uid=jjensen,ou=People,dc=example,dc=com
uid: jjensen

dn: uid=kjensen,ou=People,dc=example,dc=com
uid: kjensen

dn: uid=rjensen,ou=People,dc=example,dc=com
uid: rjensen

dn: uid=tjensen,ou=People,dc=example,dc=com
uid: tjensen


Result Code:  0 (Success)
```

You can also use `@objectclass` notation in the attribute list to return the attributes of a particular object class. The following example shows how to return attributes of the `inetOrgPerson` object class:

```
$ ldapsearch -p 1389 -b dc=example,dc=com "(uid=bjensen)" @inetorgperson
dn: uid=bjensen,ou=People,dc=example,dc=com
givenName: Barbara
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: bjensen
cn: Barbara Jensen
cn: Babs Jensen
telephoneNumber: +1 408 555 1862
sn: Jensen
roomNumber: 0209
mail: bjensen@example.com
l: San Francisco
ou: Product Development
ou: People
facsimileTelephoneNumber: +1 408 555 1992
```

You can use + in the attribute list to return all operational attributes, as in the following example:

```
$ ldapsearch -p 1389 -b dc=example,dc=com "(uid=bjensen)" +
dn: uid=bjensen,ou=People,dc=example,dc=com
numSubordinates: 0
structuralObjectClass: inetOrgPerson
etag: 0000000073c29972
subschemaSubentry: cn=schema
hasSubordinates: false
entryDN: uid=bjensen,ou=people,dc=example,dc=com
entryUUID: fc252fd9-b982-3ed6-b42a-c76d2546312c
```

ldifdiff

ldifdiff — compare small LDIF files

ldifdiff

`ldifdiff` source target

1 Description

This utility can be used to compare two LDIF files and report the differences in LDIF format.

If standard input is used to specify source or target, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

2 Options

The **ldifdiff** command takes the following options:

Command options:

`-o | --outputLDIF {file}`

Write differences to {file} instead of stdout.

Default: stdout

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

No differences were found.

1

Differences were found.

other

An error occurred.

4 Examples

The following example demonstrates use of the command with two small LDIF files.

```
$ cat /path/to/newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: changeme

$ cat /path/to/neweruser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: secret12
description: A new description.

$ ldifdiff -s /path/to/newuser.ldif -t /path/to/neweruser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
add: userPassword
userPassword: secret12
-
delete: userPassword
userPassword: changeme
-
add: description
description: A new description.
```

ldifmodify

ldifmodify — apply LDIF changes to LDIF

ldifmodify

`ldifmodify` source_file [changes_files...]

1 Description

This utility can be used to apply a set of modify, add, and delete operations to entries contained in an LDIF file.

If standard input is used to specify source or changes, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

2 Options

The **ldifmodify** command takes the following options:

Command options:

`-c | --continueOnError`

Continue processing even if there are errors.

Default: false

`-o | --outputLDIF {file}`

Write updated entries to {file} instead of stdout.

Default: stdout

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example demonstrates use of the command.

```
$ cat /path/to/newuser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: changeme

$ cat /path/to/newdiff.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
changetype: modify
add: userPassword
userPassword: secret12
-
delete: userPassword
userPassword: changeme
-
add: description
description: A new description.

$ ldifmodify -o neweruser.ldif /path/to/newuser.ldif /path/to/newdiff.ldif

$ cat neweruser.ldif
dn: uid=newuser,ou=People,dc=example,dc=com
uid: newuser
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: New User
sn: User
ou: People
mail: newuser@example.com
userPassword: secret12
description: A new description.
```

ldifsearch

ldifsearch — search LDIF with LDAP filters

ldifsearch

`ldifsearch` source filter [attributes ...]

1 Description

This utility can be used to perform search operations against entries contained in an LDIF file.

If standard input is used to specify source, end your input with EOF (Ctrl+D on UNIX, Ctrl+Z on Windows).

2 Options

The **ldifsearch** command takes the following options:

Command options:

`-A | --typesOnly`

Only retrieve attribute names but not their values.

Default: false

`-b | --baseDN {baseDN}`

The base DN for the search. If no base DN is provided, then the root DSE will be used.

Default:

`-l | --timeLimit {timeLimit}`

Maximum length of time in seconds to allow for the search.

Default: 0

`-o | --outputLDIF {file}`

Write search results to {file} instead of stdout.

Default: stdout

`-s | --searchScope {searchScope}`

Search scope ('base', 'one', 'sub', or 'subordinates'). Note: 'subordinates' is an LDAP extension that might not work with all LDAP servers.

Default: sub

`-z | --sizeLimit {sizeLimit}`

Maximum number of entries to return from the search.

Default: 0

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example demonstrates use of the command.

```
$ ldifsearch -b dc=example,dc=com Example.ldif uid=bjensen
dn: uid=bjensen,ou=People,dc=example,dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: bjensen
userpassword: hifalutin
facsimiletelephonenumber: +1 408 555 1992
givenname: Barbara
cn: Barbara Jensen
cn: Babs Jensen
telephonenumber: +1 408 555 1862
sn: Jensen
roomnumber: 0209
homeDirectory: /home/bjensen
mail: bjensen@example.com
l: San Francisco
ou: Product Development
ou: People
uidNumber: 1076
gidNumber: 1000
```

You can also use `@objectclass` notation in the attribute list to return the attributes of a particular object class. The following example shows how to return attributes of the `posixAccount` object class.

```
$ ldifsearch -b dc=example,dc=com Example.ldif "(uid=bjensen)" @posixaccount
dn: uid=bjensen,ou=People,dc=example,dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: bjensen
userpassword: hifalutin
cn: Barbara Jensen
cn: Babs Jensen
homeDirectory: /home/bjensen
uidNumber: 1076
gidNumber: 1000
```

list-backends

list-backends — list OpenDJ backends and base DNs

list-backends

```
list-backends
```

1 Description

This utility can be used to list the backends and base DNs configured in the Directory Server.

2 Options

The **list-backends** command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN for which to list the backend ID.

`-n | --backendID {backendName}`

Backend ID of the backend for which to list the base DNs.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example demonstrates a successful run.

```
$ list-backends
Backend ID         : Base DN
-------------------:---------------------
adminRoot          : cn=admin data
ads-truststore     : cn=ads-truststore
backup             : cn=backups
config             : cn=config
monitor            : cn=monitor
myCompanyRoot      : "dc=myCompany,dc=com"
myOrgRoot          : o=myOrg
schema             : cn=schema
tasks              : cn=tasks
userRoot           : "dc=example,dc=com"
```

makeldif

makeldif — generate test LDIF

makeldif

`makeldif` template-file-path

1 Description

This utility can be used to generate LDIF data based on a definition in a template file.

The *`template-file-path`* can be one of the following:

- A full path to the template file such as `/path/to/opendj/config/MakeLDIF/example.template`.
- A relative path to the template file such as `../../my-test-data.template`.
- A file name that specifies one of the template files that are built into the ${opendj.product.name.full} LDAP Toolkit, such as `example.template`, or `people_and_groups.template`.

The ${opendj.product.name.full} LDAP Toolkit includes these built-in template and data files:

`cities`

List of more than 200 cities.

`example.template`

Template to generate a base entry and users in a branch `ou=people,[suffix]`, where the default setting for suffix is `suffix=dc=example,dc=com`.

`first.names`

List of more than 8000 first names.

`last.names`

List of more than 13000 last names.

`people_and_groups.template`

Template to generate a base entry, users, and groups.

`states`

List of US states by their two-character codes.

`streets`

List of more than 70 street names.

2 Options

The **makeldif** command takes the following options:

Command options:

`-c | --constant {name=value}`

A constant that overrides the value set in the template file.

`-o | --outputLDIF {file}`

The path to the LDIF file to be written.

`-r | --resourcePath {path}`

Path to look for MakeLDIF resources (e.g., data files).

The utility looks for resources in the following locations in this order:

1. The current directory where the command is run.
2. The resource path directory.
3. The built-in files.

`-s | --randomSeed {seed}`

The seed to use to initialize the random number generator.

Default: 0

Utility input/output options:

`-t | --wrapColumn {wrapColumn}`

Maximum length of an output line (0 for no wrapping).

Default: 0

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

1

An error occurred.

4 Examples

The following example uses the default template to generate LDIF.

```
$ makeldif -o ../ldif/generated.ldif ../config/MakeLDIF/example.template
Processed 1000 entries
Processed 2000 entries
...
Processed 10000 entries
LDIF processing complete.  10003 entries written
```

5 See Also

makeldif.template(5)

makeldif.template

makeldif.template — template file for the makeldif command

makeldif.template

```
# Comment lines start with #.
#
# Notice that this synopsis includes blank lines after entries.
# In the same way you would use blank lines after entries in normal LDIF,
# leave empty lines after "entries" in template files.

# Optionally define constants used in the template.
# To reference constants later, put brackets around the name: [constant-name]
#
define constant-name=value
...

# Define branches by suffix DN, such as the following:
#
#  dc=example,dc=com
#  ou=People,dc=example,dc=com
#  ou=Groups,dc=example,dc=com
#
# makeldif generates the necessary object class definitions and RDNs.
#
# A branch can have subordinateTemplates that define templates to use for
# the branch entry. The optional number at the end
# of the subordinateTemplate specification defines how many entries to generate.
# If you do not specify a number, makeldif continues to generate entries
# indefinitely until you interrupt the command.
#
# A branch can have additional attributes generated on the branch entry. See
# the Description below for more information on specifying attribute values.
#
branch: suffix-dn
objectClass: top
objectClass: suffix-object-class
[subordinateTemplate: template-name[:number]
...]
[attribute: attr-value
...]

...

# Define entries using templates.
#
# A template can extend another template.
# A template defines the RDN attribute(s) used for generated entries.
# A template can have a subordinateTemplate that defines a template to use for
# the generated entries.
#
# A template then defines attributes. See the Description below for more
# information on specifying attribute values.
#
template: template-name
[extends: template-name]
rdnAttr: attribute[+attribute ...]
[subordinateTemplate: template-name:number]
[attribute: attr-value
```

```
...]

...
```

1 Description

Template files specify how to build LDIF. They allow you to define variables, insert random values from other files, and generally build arbitrarily large LDIF files for testing purposes. You pass template files to the **makeldif** command when generating LDIF.

The Synopsis above shows the layout for a **makeldif** template file. This section focuses on what you can do to specify entry attribute values, called *attr-value* in the Synopsis section.

Specifying Attribute Values

When specifying attribute values in **makeldif** templates, you can use static text and constants that you have defined, enclosing names for constants in brackets, `[myConstant]`. You can use more than one constant per line, as in the following example:

```
description: Description for [org] under [suffix]
```

You can also use two kinds of tags when specifying attribute values. One kind of tag is replaced with the value of another attribute in the generated entry. Such tags are delimited with braces, `{ }`. For example, if your template includes definitions for first name and last name attributes, use:

```
givenName: <first>
sn: <last>
```

Then you can define a mail attribute that uses the values of both attributes, and an initials attribute that takes the first character of each:

```
mail: {givenName}.{sn}@[myDomain]
initials: {givenName:1}{sn:1}
```

The other kind of tag is delimited with < and >, as shown above in the example with `<first>` and `<last>`. Tag names are not case sensitive. Many tags can take arguments separated by colons, `:`, from the tag names within the tag.

Use backslashes to escape literal start tag characters (`< [ {`) as shown in the following example, and to escape literal end tag characters within tags (`> ] }`):

```
scimMail: \{"emails": \[\{"value": "{mail}", "type": "work", "primary": true}]}
xml: \<id>{uid}\</id>
```

The **makeldif** command supports the following tags:

<DN>

The DN tag is replaced by the distinguished name of the current entry. An optional integer argument specifies the subcomponents of the DN to generate. For example, if the DN of the entry is `uid=bjensen,ou=People,dc=example,dc=com`, then `<DN:1>` is replaced by `uid=bjensen`, and `<DN:-2>` is replaced by `dc=example,dc=com`.

<File>

The File tag is replaced by a line from a text file you specify. The File tag takes a required argument, the path to the text file, and an optional second argument, either `random` or `sequential`. For the file argument, either specify an absolute path to the file such as `<file:/path/to/myDescriptions>`, or specify a path relative to the template file such as `<file:streets>`. For the second argument, if you specify `sequential` then lines from the file are read in sequential order. Otherwise, lines from the file are read in random order.

<First>

The first name tag is replaced by a random line from `first.names`. Combinations of generated first and last names are unique, with integers appended to the name strings if not enough combinations are available.

<GUID>

The GUID tag is replaced by a 128-bit, type 4 (random) universally unique identifier, such as `f47ac10b-58cc-4372-a567-0e02b2c3d479`.

<IfAbsent>

The IfAbsent tag takes as its first argument the name of another attribute, and optionally, as its second argument, a value to use. This tag causes the attribute to be generated only if the named attribute is not present on the generated entry. Use this tag when you have used `<Presence>` to define another attribute that is not always present on generated entries.

<IfPresent>

The IfPresent takes as its first argument the name of another attribute, and optionally, as its second argument, a value to use. This tag causes the attribute to be generated only if the named attribute is also present on the generated entry. Use this tag when you have used `<Presence>` to define another attribute that is sometimes present on generated entries.

<Last>

The last name tag is replaced by a random line from the last names template file, `last.names`. Combinations of generated first and last names are unique,

with integers appended to the name strings if not enough combinations are available.

<List>

The List tag is replaced by one of the values from the list of arguments you provide. For example, `<List:bronze:silver:gold>` is replaced with `bronze`, `silver`, or `gold`.

You can weight arguments to ensure that some arguments are selected more often than others. For example, if you want two bronze for one silver and one gold, use `<List:bronze;2:silver;1:gold;1>`.

<ParentDN>

The ParentDN tag is replaced by the distinguished name of the parent entry. For example, if the DN of the entry is `uid=bjensen,ou=People,dc=example,dc=com`, `<ParentDN>` is replaced by `ou=People,dc=example,dc=com`.

<Presence>

The Presence tag takes a percent argument. It results in the attribute value being generated or not based on the percentage of entries you specify in the argument. For example, `description: <Presence:50>A description` generates `description: A description` on half the entries.

<Random>

The Random tag lets you generate a variety of random numbers and strings. The Random tag has the following subtypes, which you include as arguments, that is `<Random:`*`subtype`*`>`:

- `alpha:`*`length`*
- `alpha:`*`min-length`*`:`*`max-length`*
- `numeric:`*`length`*
- `numeric:`*`minvalue`*`:`*`maxvalue`*
- `numeric:`*`minvalue`*`:`*`maxvalue`*`:`*`format`*, where *`format`* is a `java.text.DecimalFormat` pattern
- `alphanumeric:`*`length`*
- `alphanumeric:`*`min-length`*`:`*`max-length`*
- `chars:`*`characters`*`:`*`length`*
- `chars:`*`characters`*`:`*`min-length`*`:`*`max-length`*

- `hex:`*`length`*
- `hex:`*`min-length`*`:`*`max-length`*
- `base64:`*`length`*
- `base64:`*`min-length`*`:`*`max-length`*
- `month`
- `month:`*`max-length`*
- `telephone`, a telephone number starting with the country code `+1`

<RDN>

The RDN tag is replaced with the RDN of the entry. Use this in the template after you have specified `rdnAttr` so that the RDN has already been generated when this tag is replaced.

An optional integer argument specifies the subcomponents of the RDN to generate.

<Sequential>

The Sequential tag is replaced by a sequentially increasing generated integer. The first optional integer argument specifies the starting number. The second optional boolean argument specifies whether to start over when generating entries for a new parent entry. For example, `<Sequential>:42:true` starts counting from 42, and starts over when the parent entry changes from `o=Engineering` to `o=Marketing`.

<_DN>

The _DN tag is replaced by the DN of the current entry with underscores in the place of commas.

<_ParentDN>

The _ParentDN tag is replaced by the DN the parent entry with underscores in the place of commas.

2 Examples

The following example generates 10 organization units, each containing 50 entries. Add it next to the supporting files, such as `first.names` and `last.names` needed to generate the output:

```
define suffix=dc=example,dc=com
```

```
define maildomain=example.com
define numusers=50
define numorgs=10

branch: [suffix]
objectClass: top
objectClass: domain

branch: ou=People,[suffix]
objectClass: top
objectClass: organizationalUnit
subordinateTemplate: orgunit:[numorgs]
description: This is the People container
telephoneNumber: +33 00010002

template: orgunit
subordinateTemplate: person:[numusers]
rdnAttr: ou
ou: Org-<sequential:0>
objectClass: top
objectClass: organizationalUnit
description: This is the {ou} organizational unit

template: person
rdnAttr: uid
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
givenName: <first>
sn: <last>
cn: {givenName} {sn}
initials: {givenName:1}<random:chars:ABCDEFGHIJKLMNOPQRSTUVWXYZ:1>{sn:1}
employeeNumber: <sequential:0>
uid: user.{employeeNumber}
mail: {uid}@[maildomain]
userPassword: password
telephoneNumber: <random:telephone>
homePhone: <random:telephone>
pager: <random:telephone>
mobile: <random:telephone>
street: <random:numeric:5> <file:streets> Street
l: <file:cities>
st: <file:states>
postalCode: <random:numeric:5>
postalAddress: {cn}${street}${l}, {st}  {postalCode}
description: This is the description for {cn}.
```

3 See Also

makeldif(1), the server template file `config/MakeLDIF/example.template`

manage-account

manage-account — manage state of OpenDJ server accounts

manage-account

`manage-account` {subcommand} {options}

1 Description

This utility can be used to retrieve and manipulate the values of password policy state variables.

2 Options

The **manage-account** command takes the following options:

Command options:

`-b | --targetDN {targetDN}`

The DN of the user entry for which to get and set password policy state information.

LDAP connection options:

`-D | --bindDN {bindDN}`

The DN to use to bind to the server.

`-h | --hostname {host}`

Directory server hostname or IP address.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

The path to the file containing the bind password.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of certificate for SSL client authentication.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

The password to use to bind to the server.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Subcommands

The **manage-account** command supports the following subcommands:

3.1 manage-account clear-account-is-disabled

Clear account disabled state information from the user account.

3.2 manage-account get-account-expiration-time

Display when the user account will expire.

3.3 manage-account get-account-is-disabled

Display information about whether the user account has been administratively disabled.

3.4 manage-account get-all

Display all password policy state information for the user.

3.5 manage-account get-authentication-failure-times

Display the authentication failure times for the user.

3.6 manage-account get-grace-login-use-times

Display the grace login use times for the user.

3.7 manage-account get-last-login-time

Display the time that the user last authenticated to the server.

3.8 manage-account get-password-changed-by-required-time

Display the required password change time with which the user last complied.

3.9 manage-account get-password-changed-time

Display the time that the user's password was last changed.

3.10 manage-account get-password-expiration-warned-time

Display the time that the user first received an expiration warning notice.

3.11 manage-account get-password-history

Display password history state values for the user.

3.12 manage-account get-password-is-reset

Display information about whether the user will be required to change his or her password on the next successful authentication.

3.13 manage-account get-password-policy-dn

Display the DN of the password policy for the user.

3.14 manage-account get-remaining-authentication-failure-count

Display the number of remaining authentication failures until the user's account is locked.

3.15 manage-account get-remaining-grace-login-count

Display the number of grace logins remaining for the user.

3.16 manage-account get-seconds-until-account-expiration

Display the length of time in seconds until the user account expires.

3.17 manage-account get-seconds-until-authentication-failure-unlock

Display the length of time in seconds until the authentication failure lockout expires.

3.18 manage-account get-seconds-until-idle-lockout

Display the length of time in seconds until user's account is locked because it has remained idle for too long.

3.19 manage-account get-seconds-until-password-expiration

Display length of time in seconds until the user's password expires.

3.20 manage-account get-seconds-until-password-expiration-warning

Display the length of time in seconds until the user should start receiving password expiration warning notices.

3.21 manage-account get-seconds-until-password-reset-lockout

Display the length of time in seconds until user's account is locked because the user failed to change the password in a timely manner after an administrative reset.

3.22 manage-account get-seconds-until-required-change-time

Display the length of time in seconds that the user has remaining to change his or her password before the account becomes locked due to the required change time.

3.23 manage-account set-account-is-disabled

Specify whether the user account has been administratively disabled.

3.23.1 Options

The **manage-account set-account-is-disabled** command takes the following options:

`-O | --operationValue {true|false}`

'true' to indicate that the account is disabled, or 'false' to indicate that it is not disabled.

4 Exit Codes

0

The command completed successfully.

89

An error occurred while parsing the command-line arguments.

5 Examples

For the following examples the directory admin user, Kirsten Vaughan, has `ds-privilege-name: password-reset` and the following ACI on `ou=People,dc=example,dc=com`.

```
(target="ldap:///ou=People,dc=example,dc=com") (targetattr ="*||+")(
 version 3.0;acl "Admins can run amok"; allow(all) groupdn =
 "ldap:///cn=Directory Administrators,ou=Groups,dc=example,dc=com";)
```

The following command locks a user account.

```
$ manage-account -p 4444 -D "uid=kvaughan,ou=people,dc=example,dc=com" \
 -w bribery set-account-is-disabled -O true \
 -b uid=bjensen,ou=people,dc=example,dc=com -X
Account Is Disabled:  true
```

The following command unlocks a user account.

```
$ manage-account -p 4444 -D "uid=kvaughan,ou=people,dc=example,dc=com" \
 -w bribery clear-account-is-disabled \
 -b uid=bjensen,ou=people,dc=example,dc=com -X
Account Is Disabled:  false
```

manage-tasks

manage-tasks — manage OpenDJ server administration tasks

manage-tasks

```
manage-tasks
```

1 Description

This utility can be used to obtain a list of tasks scheduled to run within the Directory Server as well as information about individual tasks.

2 Options

The **manage-tasks** command takes the following options:

Command options:

`-c | --cancel {taskID}`

ID of a particular task to cancel.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-i | --info {taskID}`

ID of a particular task about which this tool will display information.

`-s | --summary`

Print a summary of tasks.

Default: false

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example demonstrates use of the command with a server that does daily backups at 2:00 AM.

```
$ manage-tasks -p 4444 -h opendj.example.com -D "cn=Directory Manager" \
 -w password -s

  ID                                Type    Status
  ------------------------------------------------------------
  example-backup                    Backup  Recurring
  example-backup-20110622020000000  Backup  Waiting on start time
```

rebuild-index

rebuild-index — rebuild index after configuration change

rebuild-index

```
rebuild-index
```

1 Description

This utility can be used to rebuild index data within an indexed backend database.

2 Options

The **rebuild-index** command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN of a backend supporting indexing. Rebuild is performed on indexes within the scope of the given base DN.

`--clearDegradedState`

Indicates that indexes do not need rebuilding because they are known to be empty and forcefully marks them as valid. This is an advanced option which must only be used in cases where a degraded index is known to be empty and does not therefore need rebuilding. This situation typically arises when an index is created for an attribute which has just been added to the schema.

Default: false

`-i | --index {index}`

Names of index(es) to rebuild. For an attribute index this is simply an attribute name. At least one index must be specified for rebuild. Cannot be used with the "--rebuildAll" option.

`--offline`

Indicates that the command must be run in offline mode.

Default: false

`--rebuildAll`

Rebuild all indexes, including any DN2ID, DN2URI, VLV and extensible indexes. Cannot be used with the "-i" option or the "--rebuildDegraded" option.

Default: false

`--rebuildDegraded`

Rebuild all degraded indexes, including any DN2ID, DN2URI, VLV and extensible indexes. Cannot be used with the "-i" option or the "--rebuildAll" option.

Default: false

`--tmpdirectory {directory}`

Path to temporary directory for index scratch files during index rebuilding.

Default: import-tmp

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example schedules a task to start immediately that rebuilds the `cn` (common name) index.

```
$ rebuild-index -p 4444 -h opendj.example.com -D "cn=Directory Manager" \
 -w password -b dc=example,dc=com -i cn -t 0
Rebuild Index task 20110607160349596 scheduled to start Jun 7, 2011 4:03:49 PM
```

restore

restore — restore OpenDJ directory data backups

restore

```
restore
```

1 Description

This utility can be used to restore a backup of a Directory Server backend.

2 Options

The **restore** command takes the following options:

Command options:

`-d | --backupDirectory {backupDir}`

Path to the directory containing the backup file(s).

`-I | --backupID {backupID}`

Backup ID of the backup to restore.

`-l | --listBackups`

List available backups in the backup directory.

Default: false

`-n | --dry-run`

Verify the contents of the backup but do not restore it.

Default: false

`--offline`

Indicates that the command must be run in offline mode.

Default: false

Task Backend Connection Options

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Task Scheduling Options

`--completionNotify {emailAddress}`

Email address of a recipient to be notified when the task completes. This option may be specified more than once.

`--dependency {taskID}`

ID of a task upon which this task depends. A task will not start execution until all its dependencies have completed execution.

`--errorNotify {emailAddress}`

Email address of a recipient to be notified if an error occurs when this task executes. This option may be specified more than once.

`--failedDependencyAction {action}`

Action this task will take should one if its dependent tasks fail. The value must be one of PROCESS,CANCEL,DISABLE. If not specified defaults to CANCEL.

`--recurringTask {schedulePattern}`

Indicates the task is recurring and will be scheduled according to the value argument expressed in crontab(5) compatible time/date pattern.

`-t | --start {startTime}`

Indicates the date/time at which this operation will start when scheduled as a server task expressed in YYYYMMDDhhmmssZ format for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the task to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example schedules a restore as a task to begin immediately while OpenDJ directory server is online.

```
$ restore -p 4444 -D "cn=Directory Manager" -w password
 -d /path/to/opendj/bak -I 20110613080032 -t 0
Restore task 20110613155052932 scheduled to start Jun 13, 2011 3:50:52 PM CEST
```

The following example restores data while OpenDJ is offline.

```
$ stop-ds
Stopping Server...
...

$ restore --backupDirectory /path/to/opendj/bak/userRoot \
 --listBackups
Backup ID:          20120928102414Z
Backup Date:        28/Sep/2012:12:24:17 +0200
Is Incremental:     false
Is Compressed:      false
Is Encrypted:       false
Has Unsigned Hash:  false
Has Signed Hash:    false
Dependent Upon:     none

$ restore --backupDirectory /path/to/opendj/bak/userRoot \
 --backupID 20120928102414Z
[28/Sep/2012:12:26:20 +0200] ... msg=Restored: 00000000.jdb (size 355179)

$ start-ds
[28/Sep/2012:12:27:29 +0200] ... The Directory Server has started successfully
```

setup

setup — install OpenDJ directory server

setup

```
setup
```

1 Description

This utility can be used to setup the Directory Server.

2 Options

The **setup** command takes the following options:

Command options:

`-a | --addBaseEntry`

Indicates whether to create the base entry in the Directory Server database.

Default: false

`--acceptLicense`

Automatically accepts the product license (if present).

Default: false

`--adminConnectorPort {port}`

Port on which the Administration Connector should listen for communication.

Default: 4444

`-b | --baseDN {baseDN}`

Base DN for user information in the Directory Server. Multiple base DNs may be provided by using this option multiple times.

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-d | --sampleData {numEntries}`

Specifies that the database should be populated with the specified number of sample entries.

Default: 0

`-D | --rootUserDN {rootUserDN}`

DN for the initial root user for the Directory Server.

Default: cn=Directory Manager

`--generateSelfSignedCertificate`

Generate a self-signed certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

Default: false

`-h | --hostname {host}`

The fully-qualified directory server host name that will be used when generating self-signed certificates for LDAP SSL/StartTLS, the administration connector, and replication.

Default: localhost.localdomain

`-i | --cli`

Use the command line install. If not specified the graphical interface will be launched. The rest of the options (excluding help and version) will only be taken into account if this option is specified.

Default: false

`-j | --rootUserPasswordFile {rootUserPasswordFile}`

Path to a file containing the password for the initial root user for the Directory Server.

`-l | --ldifFile {ldifFile}`

Path to an LDIF file containing data that should be added to the Directory Server database. Multiple LDIF files may be provided by using this option multiple times.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-O | --doNotStart`

Do not start the server when the configuration is completed.

Default: false

`-p | --ldapPort {port}`

Port on which the Directory Server should listen for LDAP communication.

Default: 1389

`-q | --enableStartTLS`

Enable StartTLS to allow secure communication with the server using the LDAP port.

Default: false

`-R | --rejectFile {rejectFile}`

Write rejected entries to the specified file.

`-S | --skipPortCheck`

Skip the check to determine whether the specified ports are usable.

Default: false

`--skipFile {skipFile}`

Write skipped entries to the specified file.

`-t | --backendType {backendType}`

The type of the userRoot backend.

Default: `je` for standard edition, `pdb` for OEM edition.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate (JKS, JCEKS, PKCS#12 or PKCS#11) as server certificate.

`--useBcfksKeystore {keyStorePath}`

Path of a BCFKS key store containing the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`--useJavaKeystore {keyStorePath}`

Path of a Java Key Store (JKS) containing a certificate to be used as the server certificate. This does not apply to the administration connector, which uses its own key store and certificate (default: config/admin-keystore and admin-cert).

`--useJCEKS {keyStorePath}`

Path of a JCEKS containing a certificate to be used as the server certificate.

`--usePkcs11Keystore`

Use a certificate in a PKCS#11 token that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

Default: false

`--usePkcs12keyStore {keyStorePath}`

Path of a PKCS#12 key store containing the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-w | --rootUserPassword {rootUserPassword}`

Password for the initial root user for the Directory Server.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate (JKS, JCEKS, PKCS#12 or PKCS#11) as server certificate.

`-x | --jmxPort {jmxPort}`

Port on which the Directory Server should listen for JMX communication.

Default: 1689

`-Z | --ldapsPort {port}`

Port on which the Directory Server should listen for LDAPS communication. The LDAPS port will be configured and SSL will be enabled only if this argument is explicitly specified.

Default: 1636

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following command installs OpenDJ directory server, enabling StartTLS and importing 100 example entries without interaction.

```
$ /path/to/opendj/setup --cli -b dc=example,dc=com -d 100 \
 -D "cn=Directory Manager" -w password -h opendj.example.com -p 1389 \
 --generateSelfSignedCertificate --enableStartTLS -n

OpenDJ version
 Please wait while the setup program initializes...

See /var/.../opends-setup-484...561.log for a detailed log of this operation.

Configuring Directory Server ..... Done.
Configuring Certificates ..... Done.
Importing Automatically-Generated Data (100 Entries) ......... Done.
Starting Directory Server .......... Done.

To see basic server configuration status and configuration, you can launch
 /path/to/opendj/bin/status
```

start-ds

start-ds — start OpenDJ directory server

start-ds

```
start-ds
```

1 Description

This utility can be used to start the Directory Server, as well as to obtain the server version and other forms of general server information.

2 Options

The **start-ds** command takes the following options:

Command options:

`-L | --useLastKnownGoodConfig`

Attempt to start using the configuration that was in place at the last successful startup (if it is available) rather than using the current active configuration.

Default: false

`-N | --nodetach`

Do not detach from the terminal and continue running in the foreground. This option cannot be used with the -t, --timeout option.

Default: false

`-s | --systemInfo`

Display general system information.

Default: false

`-t | --timeout {seconds}`

Maximum time (in seconds) to wait before the command returns (the server continues the startup process, regardless). A value of '0' indicates an infinite timeout, which means that the command returns only when the server startup is completed. The default value is 60 seconds. This option cannot be used with the -N, --nodetach option.

Default: 200

Utility input/output options:

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following command starts the server without displaying information about the startup process.

```
$ start-ds -Q
```

status

status — display basic OpenDJ server information

status

`status` {options}

1 Description

This utility can be used to display basic server information.

2 Options

The **status** command takes the following options:

Command options:

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

Default: cn=Directory Manager

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-r | --refresh {period}`

When this argument is specified, the status command will display its contents periodically. Used to specify the period (in seconds) between two displays of the status.

`-s | --script-friendly`

Use script-friendly mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

```
$ status -D "cn=Directory Manager" -w password

          --- Server Status ---
Server Run Status:        Started
Open Connections:         1

          --- Server Details ---
Host Name:                localhost.localdomain
Administrative Users:     cn=Directory Manager
Installation Path:        /path/to/opendj
Version:                  OpenDJ version
Java Version:             version
Administration Connector: Port 4444 (LDAPS)

          --- Connection Handlers ---
Address:Port : Protocol    : State
-------------:-------------:---------
--           : LDIF        : Disabled
8989         : Replication : Enabled
0.0.0.0:161  : SNMP        : Disabled
0.0.0.0:636  : LDAPS       : Disabled
0.0.0.0:1389 : LDAP        : Enabled
0.0.0.0:1689 : JMX         : Disabled

          --- Data Sources ---
Base DN:                      dc=example,dc=com
Backend ID:                   userRoot
Entries:                      160
Replication:                  Enabled
Missing Changes:              0
Age of Oldest Missing Change: <not available>

Base DN:     dc=myCompany,dc=com
Backend ID:  myCompanyRoot
Entries:     3
Replication: Disabled

Base DN:     o=myOrg
Backend ID:  myOrgRoot
Entries:     3
Replication: Disabled
```

stop-ds

stop-ds — stop OpenDJ directory server

stop-ds

```
stop-ds
```

1 Description

This utility can be used to request that the Directory Server stop running or perform a restart. When run without connection options, this utility sends a signal to the OpenDJ process to stop the server. When run with connection options, this utility connects to the OpenDJ administration port and creates a shutdown task to stop the server.

2 Options

The **stop-ds** command takes the following options:

Command options:

`-r | --stopReason {stopReason}`

Reason the server is being stopped or restarted.

`-R | --restart`

Attempt to automatically restart the server once it has stopped.

Default: false

`-t | --stopTime {stopTime}`

Indicates the date/time at which the shutdown operation will begin as a server task expressed in format YYYYMMDDhhmmssZ for UTC time or YYYYMMDDhhmmss for local time. A value of '0' will cause the shutdown to be scheduled for immediate execution. When this option is specified the operation will be scheduled to start at the specified time after which this utility will exit immediately.

`-Y | --proxyAs {authzID}`

Use the proxied authorization control with the given authorization ID.

LDAP connection options:

`-D | --bindDN {bindDN}`

DN to use to bind to the server.

`-h | --hostname {host}`

Directory server hostname or IP address.

Default: localhost.localdomain

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of certificate for SSL client authentication.

`-o | --saslOption {name=value}`

SASL bind options.

`-p | --port {port}`

Directory server administration port number.

Default: 4444

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following example restarts OpenDJ directory server.

```
$ stop-ds --restart
Stopping Server...

...The Directory Server has started successfully
```

uninstall

uninstall — remove OpenDJ directory server software

uninstall

`uninstall` {options}

1 Description

This utility can be used to uninstall the Directory Server.

2 Options

The **uninstall** command takes the following options:

Command options:

`-a | --remove-all`

Remove all components of the server (this option is not compatible with the rest of remove options).

Default: false

`-b | --backup-files`

Remove backup files.

Default: false

`-c | --configuration-files`

Remove configuration files.

Default: false

`--connectTimeout {timeout}`

Maximum length of time (in milliseconds) that can be taken to establish a connection. Use '0' to specify no time out.

Default: 30000

`-d | --databases`

Remove database contents.

Default: false

`-e | --ldif-files`

Remove LDIF files.

Default: false

`-f | --forceOnError`

Specifies whether the uninstall should continue if there is an error updating references to this server in remote server instances or not. This option can only be used with the --no-prompt no prompt option.

Default: false

`-i | --cli`

Use the command line install. If not specified the graphical interface will be launched. The rest of the options (excluding help and version) will only be taken into account if this option is specified.

Default: false

`-l | --server-libraries`

Remove Server Libraries and Administrative Tools.

Default: false

`-L | --log-files`

Remove log files.

Default: false

LDAP connection options:

`-h | --referencedHostName {host}`

The name of this host (or IP address) as it is referenced in remote servers for replication.

Default: localhost.localdomain

`-I | --adminUID {adminUID}`

User ID of the Global Administrator to use to bind to the server.

Default: admin

`-j | --bindPasswordFile {bindPasswordFile}`

Bind password file.

`-K | --keyStorePath {keyStorePath}`

Certificate key store path.

`-N | --certNickname {nickname}`

Nickname of the certificate that the server should use when accepting SSL-based connections or performing StartTLS negotiation.

`-o | --saslOption {name=value}`

SASL bind options.

`-P | --trustStorePath {trustStorePath}`

Certificate trust store path.

`-T | --trustStorePassword {trustStorePassword}`

Certificate trust store PIN.

`-u | --keyStorePasswordFile {keyStorePasswordFile}`

Certificate key store PIN file. A PIN is required when you specify to use an existing certificate as server certificate.

`-U | --trustStorePasswordFile {path}`

Certificate trust store PIN file.

`-w | --bindPassword {bindPassword}`

Password to use to bind to the server. Use -w - to ensure that the command prompts for the password, rather than entering the password as a command argument.

`-W | --keyStorePassword {keyStorePassword}`

Certificate key store PIN. A PIN is required when you specify to use an existing certificate as server certificate.

`-X | --trustAll`

Trust all server SSL certificates.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`--noPropertiesFile`

No properties file will be used to get default command line argument values.

Default: false

`--propertiesFilePath {propertiesFilePath}`

Path to the file containing default property values used for command line arguments.

`-Q | --quiet`

Use quiet mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

4 Examples

The following command removes OpenDJ directory server without interaction.

```
$ /path/to/opendj/uninstall -a --cli -I admin -w password -n

Stopping Directory Server ..... Done.
Deleting Files under the Installation Path ..... Done.

The Uninstall Completed Successfully.
To complete the uninstallation, you must delete manually the following files
and directories:
/path/to/opendj/lib
See /var/.../opends-uninstall-3...0.log for a detailed log of this operation.

$ rm -rf /path/to/opendj
```

upgrade

upgrade — upgrade OpenDJ configuration and application data

upgrade

`upgrade` {options}

1 Description

Upgrades OpenDJ configuration and application data so that it is compatible with the installed binaries.

This tool should be run immediately after upgrading the OpenDJ binaries and before restarting the server.

NOTE: this tool does not provide backup or restore capabilities. Therefore, it is the responsibility of the OpenDJ administrator to take necessary precautions before performing the upgrade.

This utility thus performs only part of the upgrade process, which includes the following phases for a single server.

1. Get and unpack a newer version of OpenDJ directory server software.
2. Stop the current OpenDJ directory server.
3. Overwrite existing binary and script files with those of the newer version, and then run this utility before restarting OpenDJ.
4. Start the upgraded OpenDJ directory server.

Important

This utility *does not back up OpenDJ before you upgrade, nor does it restore OpenDJ if the utility fails*. In order to revert a failed upgrade, make sure you back up OpenDJ directory server before you overwrite existing binary and script files.

By default this utility requests confirmation before making important configuration changes. You can use the `--no-prompt` option to run the command non-interactively.

When using the `--no-prompt` option, if this utility cannot complete because it requires confirmation for a potentially very long or critical task, then it exits with an error and a message about how to finish making the changes. You can add the `--force` option to force a non-interactive upgrade to continue in this case, also performing long running and critical tasks.

After upgrading, see the resulting `upgrade.log` file for a full list of operations performed.

2 Options

The **upgrade** command takes the following options:

Command options:

`--acceptLicense`

Automatically accepts the product license (if present).

Default: false

`--force`

Forces a non-interactive upgrade to continue even if it requires user interaction. In particular, long running or critical upgrade tasks, such as re-indexing, which require user confirmation will be skipped. This option may only be used with the 'no-prompt' option.

Default: false

`--ignoreErrors`

Ignores any errors which occur during the upgrade. This option should be used with caution and may be useful in automated deployments where potential errors are known in advance and resolved after the upgrade has completed.

Default: false

Utility input/output options:

`-n | --no-prompt`

Use non-interactive mode. If data in the command is missing, the user is not prompted and the tool will fail.

Default: false

`-Q | --quiet`

Use quiet mode.

Default: false

`-v | --verbose`

Use verbose mode.

Default: false

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

2

The command was run in non-interactive mode, but could not complete because confirmation was required to run a long or critical task.

See the error message or the log for details.

other

An error occurred.

See the *OpenDJ Installation Guide* for an example upgrade process for OpenDJ directory server installed from the cross-platform (.zip) delivery.

Native packages (.deb, .rpm) perform more of the upgrade process, stopping OpenDJ if it is running, overwriting older files with newer files, running this utility, and starting OpenDJ if it was running when you upgraded the package(s).

verify-index

verify-index — check index for consistency or errors

verify-index

```
verify-index
```

1 Description

This utility can be used to ensure that index data is consistent within an indexed backend database.

2 Options

The **verify-index** command takes the following options:

Command options:

`-b | --baseDN {baseDN}`

Base DN of a backend supporting indexing. Verification is performed on indexes within the scope of the given base DN.

`-c | --clean`

Specifies that a single index should be verified to ensure it is clean. An index is clean if each index value references only entries containing that value. Only one index at a time may be verified in this way.

Default: false

`--countErrors`

Count the number of errors found during the verification and return that value as the exit code (values > 255 will be reduced to 255 due to exit code restrictions).

Default: false

`-i | --index {index}`

Name of an index to be verified. For an attribute index this is simply an attribute name. Multiple indexes may be verified for completeness, or all indexes if no indexes are specified. An index is complete if each index value references all entries containing that value.

General options:

`-V | --version`

Display Directory Server version information.

Default: false

`-H | --help`

Display this usage information.

Default: false

3 Exit Codes

0

The command completed successfully.

1

The command was run in non-interactive mode, but could not complete because confirmation was required to run a long or critical task.

See the error message or the log for details.

0-255

The number of errors in the index, as indicated for the `--countErrors` option.

4 Examples

The following example shows how to verify the `sn` (surname) index for completeness and for errors. The messages shown are for a backend of type `pdb`. The output is similar for other backend types:

```
$ verify-index -b dc=example,dc=com -i sn --clean --countErrors
[20/05/2015:14:24:18 +0200] category=...PDBStorage seq=0 severity=INFO
 msg=The PDB storage for backend 'userRoot' initialized
 to use 57528 buffers of 16384 bytes (total 920448kb)
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=1 severity=INFO
 msg=Checked 478 records and found 0 error(s) in 0 seconds
 (average rate 3594.0/sec)
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=2 severity=FINE
 msg=Number of records referencing more than one entry: 224
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=3 severity=FINE
 msg=Number of records that exceed the entry limit: 0
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=4 severity=FINE
 msg=Average number of entries referenced is 2.00/record
[20/05/2015:14:24:18 +0200] category=...pluggable.VerifyJob seq=5 severity=FINE
 msg=Maximum number of entries referenced by any record is 32
```

windows-service

windows-service — register OpenDJ as a Windows Service

windows-service

`windows-service` {options}

1 Description

This utility can be used to run OpenDJ directory server as a Windows Service.

2 Service Options

`-c, --cleanupService` *`serviceName`*

Disable the service and clean up the windows registry information associated with the provided service name

`-d, --disableService`

Disable the server as a Windows service and stop the server

`-e, --enableService`

Enable the server as a Windows service

`-s, --serviceState`

Provide information about the state of the server as a Windows service

3 General Options

`-V, --version`

Display version information

`-?, -H, --help`

Display usage information

4 Exit Codes

0

The command completed successfully.

> 0

An error occurred.

5 Example

The following command registers OpenDJ directory server as a Windows Service.

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

After running this command, you can manage the service using Windows administration tools.

dsconfig Subcommands Reference

This section covers **dsconfig** subcommands.

Table of Contents

dsconfig create-access-log-filtering-criteria

dsconfig create-access-log-filtering-criteria — Creates Access Log Filtering Criteria

dsconfig create-access-log-filtering-criteria

`dsconfig create-access-log-filtering-criteria` {options}

1 Description

Creates Access Log Filtering Criteria.

2 Options

The **dsconfig create-access-log-filtering-criteria** command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the new Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

3 Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-account-status-notification-handler

dsconfig create-account-status-notification-handler — Creates Account Status Notification Handlers

dsconfig create-account-status-notification-handler

```
dsconfig create-account-status-notification-handler {options}
```

1 Description

Creates Account Status Notification Handlers.

2 Options

The **dsconfig create-account-status-notification-handler** command takes the following options:

`--handler-name {name}`

The name of the new Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Account Status Notification Handler which should be created. The value for TYPE can be one of: custom | error-log | smtp.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {type}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {type}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

3 Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-alert-handler

dsconfig create-alert-handler — Creates Alert Handlers

dsconfig create-alert-handler

```
dsconfig create-alert-handler {options}
```

1 Description

Creates Alert Handlers.

2 Options

The **dsconfig create-alert-handler** command takes the following options:

`--handler-name {name}`

The name of the new Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {name}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {name}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Alert Handler which should be created. The value for TYPE can be one of: custom | jmx | smtp.

Alert Handler properties depend on the Alert Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {type}: JMX Alert Handler

Enabled by default: true

See the section called "JMX Alert Handler" for the properties of this Alert Handler type.

smtp-alert-handler

Default {type}: SMTP Alert Handler

Enabled by default: true

See the section called "SMTP Alert Handler" for the properties of this Alert Handler type.

3 JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-backend

dsconfig create-backend — Creates Backends

dsconfig create-backend

```
dsconfig create-backend {options}
```

1 Description

Creates Backends.

2 Options

The **dsconfig create-backend** command takes the following options:

`--backend-name {STRING}`

The name of the new Backend which will also be used as the value of the "backend-id" property: Specifies a name to identify the associated backend.

Backend properties depend on the Backend type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {STRING}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {STRING}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {STRING}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {STRING}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {STRING}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {STRING}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {STRING}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {STRING}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {STRING}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {STRING}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {STRING}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend properties depend on the Backend type, which depends on the `--backend-name {STRING}` option.

`-t | --type {type}`

The type of Backend which should be created. The value for TYPE can be one of: backup | cas | custom | custom-local | je | ldif | memory | monitor | null | pdb | schema | task | trust-store.

Backend properties depend on the Backend type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {type}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {type}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {type}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {type}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {type}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {type}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {type}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {type}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {type}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {type}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {type}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

3 Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the

operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these

default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the

operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

5 JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an

algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be

used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes

that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk

is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to

the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

10 PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE

(which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-backend-index

dsconfig create-backend-index — Creates Backend Indexes

dsconfig create-backend-index

```
dsconfig create-backend-index {options}
```

1 Description

Creates Backend Indexes.

2 Options

The **dsconfig create-backend-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--index-name {OID}`

The name of the new Backend Index which will also be used as the value of the "attribute" property: Specifies the name of the attribute for which the index is to be maintained.

Backend Index properties depend on the Backend Index type, which depends on the {OID} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {OID}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {OID}` option.

3 Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-backend-vlv-index

dsconfig create-backend-vlv-index — Creates Backend VLV Indexes

dsconfig create-backend-vlv-index

```
dsconfig create-backend-vlv-index {options}
```

1 Description

Creates Backend VLV Indexes.

2 Options

The **dsconfig create-backend-vlv-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--index-name {STRING}`

The name of the new Backend VLV Index which will also be used as the value of the "name" property: Specifies a unique name for this VLV index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {STRING}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {STRING}` option.

3 Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

The VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig create-certificate-mapper

dsconfig create-certificate-mapper — Creates Certificate Mappers

dsconfig create-certificate-mapper

```
dsconfig create-certificate-mapper {options}
```

1 Description

Creates Certificate Mappers.

2 Options

The **dsconfig create-certificate-mapper** command takes the following options:

`--mapper-name {name}`

The name of the new Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`-t | --type {type}`

The type of Certificate Mapper which should be created. The value for TYPE can be one of: custom | fingerprint | subject-attribute-to-user-attribute | subject-dn-to-user-attribute | subject-equals-dn.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {type}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {type}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {type}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {type}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

3 Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-connection-handler

dsconfig create-connection-handler — Creates Connection Handlers

dsconfig create-connection-handler

```
dsconfig create-connection-handler {options}
```

1 Description

Creates Connection Handlers.

2 Options

The **dsconfig create-connection-handler** command takes the following options:

`--handler-name {name}`

The name of the new Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {name}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {name}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {name}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {name}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {name}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Connection Handler which should be created. The value for TYPE can be one of: custom | http | jmx | ldap | ldif | snmp.

Connection Handler properties depend on the Connection Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {type}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {type}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {type}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {type}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {type}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

3 HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a

very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple

addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept

new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

5 LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure

channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message

may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig create-debug-target

dsconfig create-debug-target — Creates Debug Targets

dsconfig create-debug-target

```
dsconfig create-debug-target {options}
```

1 Description

Creates Debug Targets.

2 Options

The **dsconfig create-debug-target** command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--target-name {STRING}`

The name of the new Debug Target which will also be used as the value of the "debug-scope" property: Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Debug Target properties depend on the Debug Target type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {STRING}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {STRING}` option.

3 Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-entry-cache

dsconfig create-entry-cache — Creates Entry Caches

dsconfig create-entry-cache

```
dsconfig create-entry-cache {options}
```

1 Description

Creates Entry Caches.

2 Options

The **dsconfig create-entry-cache** command takes the following options:

`--cache-name {name}`

The name of the new Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {name}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`-t | --type {type}`

The type of Entry Cache which should be created. The value for TYPE can be one of: custom | fifo | soft-reference.

Entry Cache properties depend on the Entry Cache type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {type}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {type}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

3 FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very

low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-extended-operation-handler

dsconfig create-extended-operation-handler — Creates Extended Operation Handlers

dsconfig create-extended-operation-handler

```
dsconfig create-extended-operation-handler {options}
```

1 Description

Creates Extended Operation Handlers.

2 Options

The **dsconfig create-extended-operation-handler** command takes the following options:

`--handler-name {name}`

The name of the new Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of Extended Operation Handler which should be created. The value for TYPE can be one of: cancel | custom | get-connection-id | get-symmetric-key | password-modify | password-policy-state | start-tls | who-am-i.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {type}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {type}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {type}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {type}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {type}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {type}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {type}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

3 Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-group-implementation

dsconfig create-group-implementation — Creates Group Implementations

dsconfig create-group-implementation

```
dsconfig create-group-implementation {options}
```

1 Description

Creates Group Implementations.

2 Options

The **dsconfig create-group-implementation** command takes the following options:

`--implementation-name {name}`

The name of the new Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {name}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {name}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`-t | --type {type}`

The type of Group Implementation which should be created. The value for TYPE can be one of: custom | dynamic | static | virtual-static.

Group Implementation properties depend on the Group Implementation type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {type}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {type}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {type}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

3 Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-http-authorization-mechanism

dsconfig create-http-authorization-mechanism — Creates HTTP Authorization Mechanisms

dsconfig create-http-authorization-mechanism

```
dsconfig create-http-authorization-mechanism {options}
```

1 Description

Creates HTTP Authorization Mechanisms.

2 Options

The **dsconfig create-http-authorization-mechanism** command takes the following options:

`--mechanism-name {name}`

The name of the new HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`-t | --type {type}`

The type of HTTP Authorization Mechanism which should be created. The value for TYPE can be one of: http-anonymous-authorization-mechanism | http-basic-authorization-mechanism | http-oauth2-cts-authorization-mechanism | http-oauth2-file-authorization-mechanism | http-oauth2-openam-

authorization-mechanism | http-oauth2-token-introspection-authorization-mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {type}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {type}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {type}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {type}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {type}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {type}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

3 HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

8 HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationM

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig create-http-endpoint

dsconfig create-http-endpoint — Creates HTTP Endpoints

dsconfig create-http-endpoint

```
dsconfig create-http-endpoint {options}
```

1 Description

Creates HTTP Endpoints.

2 Options

The **dsconfig create-http-endpoint** command takes the following options:

`--endpoint-name {STRING}`

The name of the new HTTP Endpoint which will also be used as the value of the "base-path" property: All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {STRING} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {STRING}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {STRING}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {STRING}` option.

`-t | --type {type}`

The type of HTTP Endpoint which should be created (Default: generic). The value for TYPE can be one of: admin-endpoint | generic | rest2ldap-endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {type}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {type}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

3 Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-identity-mapper

dsconfig create-identity-mapper — Creates Identity Mappers

dsconfig create-identity-mapper

```
dsconfig create-identity-mapper {options}
```

1 Description

Creates Identity Mappers.

2 Options

The **dsconfig create-identity-mapper** command takes the following options:

`--mapper-name {name}`

The name of the new Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`-t | --type {type}`

The type of Identity Mapper which should be created. The value for TYPE can be one of: custom | exact-match | regular-expression.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {type}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {type}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

3 Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided

ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/

cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-key-manager-provider

dsconfig create-key-manager-provider — Creates Key Manager Providers

dsconfig create-key-manager-provider

```
dsconfig create-key-manager-provider {options}
```

1 Description

Creates Key Manager Providers.

2 Options

The **dsconfig create-key-manager-provider** command takes the following options:

`--provider-name {name}`

The name of the new Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {name}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Key Manager Provider which should be created. The value for TYPE can be one of: custom | file-based | ldap | pkcs11.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {type}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {type}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {type}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

3 File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

5 PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig create-log-publisher

dsconfig create-log-publisher — Creates Log Publishers

dsconfig create-log-publisher

```
dsconfig create-log-publisher {options}
```

1 Description

Creates Log Publishers.

2 Options

The **dsconfig create-log-publisher** command takes the following options:

`--publisher-name {name}`

The name of the new Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {name}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {name}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {name}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {name}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`-t | --type {type}`

The type of Log Publisher which should be created. The value for TYPE can be one of: csv-file-access | csv-file-http-access | custom-access | custom-debug | custom-error | custom-http-access | external-access | external-http-access | file-based-access | file-based-audit | file-based-debug | file-based-error | file-based-http-access | json-file-access | json-file-http-access.

Log Publisher properties depend on the Log Publisher type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {type}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {type}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {type}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {type}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {type}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {type}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {type}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {type}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {type}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {type}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {type}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

3 Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error

warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control,

admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

11 File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true OpenDJ

supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

12 Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-log-retention-policy

dsconfig create-log-retention-policy — Creates Log Retention Policies

dsconfig create-log-retention-policy

`dsconfig create-log-retention-policy {options}`

1 Description

Creates Log Retention Policies.

2 Options

The **dsconfig create-log-retention-policy** command takes the following options:

`--policy-name {name}`

The name of the new Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {name}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`-t | --type {type}`

The type of Log Retention Policy which should be created. The value for TYPE can be one of: custom | file-count | free-disk-space | size-limit.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {type}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {type}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {type}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

3 File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-log-rotation-policy

dsconfig create-log-rotation-policy — Creates Log Rotation Policies

dsconfig create-log-rotation-policy

`dsconfig create-log-rotation-policy {options}`

1 Description

Creates Log Rotation Policies.

2 Options

The **dsconfig create-log-rotation-policy** command takes the following options:

`--policy-name {name}`

The name of the new Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`-t | --type {type}`

The type of Log Rotation Policy which should be created. The value for TYPE can be one of: custom | fixed-time | size-limit | time-limit.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {type}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {type}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {type}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

3 Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-monitor-provider

dsconfig create-monitor-provider — Creates Monitor Providers

dsconfig create-monitor-provider

```
dsconfig create-monitor-provider {options}
```

1 Description

Creates Monitor Providers.

2 Options

The **dsconfig create-monitor-provider** command takes the following options:

`--provider-name {name}`

The name of the new Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {name}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {name}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Monitor Provider which should be created. The value for TYPE can be one of: client-connection | custom | entry-cache | memory-usage | stack-trace | system-info | version.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {type}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {type}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {type}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {type}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {type}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {type}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

3 Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-password-generator

dsconfig create-password-generator — Creates Password Generators

dsconfig create-password-generator

```
dsconfig create-password-generator {options}
```

1 Description

Creates Password Generators.

2 Options

The **dsconfig create-password-generator** command takes the following options:

`--generator-name {name}`

The name of the new Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {name}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`-t | --type {type}`

The type of Password Generator which should be created. The value for TYPE can be one of: custom | random.

Password Generator properties depend on the Password Generator type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {type}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

3 Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-password-policy

dsconfig create-password-policy — Creates Authentication Policies

dsconfig create-password-policy

```
dsconfig create-password-policy {options}
```

1 Description

Creates Authentication Policies.

2 Options

The **dsconfig create-password-policy** command takes the following options:

`--policy-name {name}`

The name of the new Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {name}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

`-t | --type {type}`

The type of Authentication Policy which should be created. The value for TYPE can be one of: ldap-pass-through | password-policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {type}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {type}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

3 LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be

composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds

- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they

become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity

or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-password-storage-scheme

dsconfig create-password-storage-scheme — Creates Password Storage Schemes

dsconfig create-password-storage-scheme

```
dsconfig create-password-storage-scheme {options}
```

1 Description

Creates Password Storage Schemes.

2 Options

The **dsconfig create-password-storage-scheme** command takes the following options:

`--scheme-name {name}`

The name of the new Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {name}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`-t | --type {type}`

The type of Password Storage Scheme which should be created. The value for TYPE can be one of: aes | base64 | bcrypt | blowfish | clear | crypt | custom

| md5 | pbkdf2 | pbkdf2-hmac-sha256 | pbkdf2-hmac-sha512 | pkcs5s2 | rc4 | salted-md5 | salted-sha1 | salted-sha256 | salted-sha384 | salted-sha512 | sha1 | triple-des.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {type}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {type}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {type}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {type}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {type}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {type}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {type}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {type}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {type}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {type}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {type}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {type}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {type}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {type}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {type}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {type}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {type}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {type}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

3 AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

15 Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

16 Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

17 Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

18 Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

19 SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

20 Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-password-validator

dsconfig create-password-validator — Creates Password Validators

dsconfig create-password-validator

```
dsconfig create-password-validator {options}
```

1 Description

Creates Password Validators.

2 Options

The **dsconfig create-password-validator** command takes the following options:

`--validator-name {name}`

The name of the new Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {name}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {name}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {name}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {name}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {name}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {name}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`-t | --type {type}`

The type of Password Validator which should be created. The value for TYPE can be one of: attribute-value | character-set | custom | dictionary | length-based | repeated-characters | similarity-based | unique-characters.

Password Validator properties depend on the Password Validator type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {type}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {type}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {type}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {type}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {type}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {type}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {type}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

3 Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters

from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those

requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects

a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-plugin

dsconfig create-plugin — Creates Plugins

dsconfig create-plugin

```
dsconfig create-plugin {options}
```

1 Description

Creates Plugins.

2 Options

The **dsconfig create-plugin** command takes the following options:

`--plugin-name {name}`

The name of the new Plugin.

Plugin properties depend on the Plugin type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {name}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {name}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {name}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {name}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {name}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {name}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {name}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {name}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {name}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`-t | --type {type}`

The type of Plugin which should be created. The value for TYPE can be one of: attribute-cleanup | change-number-control | custom | entry-uuid |

fractional-ldif-import | last-mod | ldap-attribute-description-list | password-policy-import | profiler | referential-integrity | samba-password | seven-bit-clean | unique-attribute.

Plugin properties depend on the Plugin type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {type}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {type}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {type}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {type}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {type}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {type}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {type}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {type}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {type}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {type}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {type}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {type}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

3 Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd

preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that

it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd

postOperationDelete

postOperationModify

postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

7 Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that

it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password

syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Changes to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

11 Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete

postoperationmodifydn

subordinatemodifydn

subordinatedelete

preoperationadd

preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify

postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid

mail

userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preparseadd

preparsemodify

preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

postoperationadd

postoperationmodify

postoperationmodifydn

postsynchronizationadd

postsynchronizationmodify

postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-replication-domain

dsconfig create-replication-domain — Creates Replication Domains

dsconfig create-replication-domain

```
dsconfig create-replication-domain {options}
```

1 Description

Creates Replication Domains.

2 Options

The **dsconfig create-replication-domain** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the new Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

3 Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-replication-server

dsconfig create-replication-server — Creates Replication Servers

dsconfig create-replication-server

```
dsconfig create-replication-server {options}
```

1 Description

Creates Replication Servers.

2 Options

The **dsconfig create-replication-server** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {name}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

3 Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some

cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new

monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-sasl-mechanism-handler

dsconfig create-sasl-mechanism-handler — Creates SASL Mechanism Handlers

dsconfig create-sasl-mechanism-handler

```
dsconfig create-sasl-mechanism-handler {options}
```

1 Description

Creates SASL Mechanism Handlers.

2 Options

The **dsconfig create-sasl-mechanism-handler** command takes the following options:

`--handler-name {name}`

The name of the new SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`-t | --type {type}`

The type of SASL Mechanism Handler which should be created. The value for TYPE can be one of: anonymous | cram-md5 | custom | digest-md5 | external | gssapi | plain.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {type}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {type}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {type}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {type}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {type}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {type}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

3 Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the

server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization

ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-schema-provider

dsconfig create-schema-provider — Creates Schema Providers

dsconfig create-schema-provider

```
dsconfig create-schema-provider {options}
```

1 Description

Creates Schema Providers.

2 Options

The **dsconfig create-schema-provider** command takes the following options:

`--provider-name {name}`

The name of the new Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {name}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {name}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Schema Provider which should be created (Default: generic). The value for TYPE can be one of: core-schema | generic | json-schema.

Schema Provider properties depend on the Schema Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {type}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {type}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

3 Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '*' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig create-service-discovery-mechanism

dsconfig create-service-discovery-mechanism — Creates Service Discovery Mechanisms

dsconfig create-service-discovery-mechanism

```
dsconfig create-service-discovery-mechanism {options}
```

1 Description

Creates Service Discovery Mechanisms.

2 Options

The **dsconfig create-service-discovery-mechanism** command takes the following options:

`--mechanism-name {name}`

The name of the new Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`-t | --type {type}`

The type of Service Discovery Mechanism which should be created (Default: generic). The value for TYPE can be one of: generic | replication | static.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {type}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {type}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

3 Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

4 Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig create-synchronization-provider

dsconfig create-synchronization-provider — Creates Synchronization Providers

dsconfig create-synchronization-provider

```
dsconfig create-synchronization-provider {options}
```

1 Description

Creates Synchronization Providers.

2 Options

The **dsconfig create-synchronization-provider** command takes the following options:

`--provider-name {name}`

The name of the new Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {name}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Synchronization Provider which should be created. The value for TYPE can be one of: custom | replication.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {type}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

3 Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- w: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig create-trust-manager-provider

dsconfig create-trust-manager-provider — Creates Trust Manager Providers

dsconfig create-trust-manager-provider

```
dsconfig create-trust-manager-provider {options}
```

1 Description

Creates Trust Manager Providers.

2 Options

The **dsconfig create-trust-manager-provider** command takes the following options:

`--provider-name {name}`

The name of the new Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`-t | --type {type}`

The type of Trust Manager Provider which should be created. The value for TYPE can be one of: blind | custom | file-based | ldap | pkcs11.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {type}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {type}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {type}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {type}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

3 Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

6 PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig create-virtual-attribute

dsconfig create-virtual-attribute — Creates Virtual Attributes

dsconfig create-virtual-attribute

```
dsconfig create-virtual-attribute {options}
```

1 Description

Creates Virtual Attributes.

2 Options

The **dsconfig create-virtual-attribute** command takes the following options:

`--name {name}`

The name of the new Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {name}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`-t | --type {type}`

The type of Virtual Attribute which should be created. The value for TYPE can be one of: collective-attribute-subentries | custom | entity-tag | entry-dn | entry-uuid | governing-structure-rule | has-subordinates | is-member-of | member | num-subordinates | password-expiration-time | password-policy-subentry | structural-object-class | subschema-subentry | user-defined.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {type} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {type}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {type}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {type}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {type}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {type}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {type}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {type}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {type}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {type}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {type}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {type}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {type}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {type}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {type}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

3 Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

10 Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

14 Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

15 Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

16 User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-access-log-filtering-criteria

dsconfig delete-access-log-filtering-criteria — Deletes Access Log Filtering Criteria

dsconfig delete-access-log-filtering-criteria

```
dsconfig delete-access-log-filtering-criteria {options}
```

1 Description

Deletes Access Log Filtering Criteria.

2 Options

The **dsconfig delete-access-log-filtering-criteria** command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`-f | --force`

Ignore non-existent Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default null: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

3 Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces

either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN

components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-account-status-notification-handler

dsconfig delete-account-status-notification-handler — Deletes Account Status Notification Handlers

dsconfig delete-account-status-notification-handler

```
dsconfig delete-account-status-notification-handler {options}
```

1 Description

Deletes Account Status Notification Handlers.

2 Options

The **dsconfig delete-account-status-notification-handler** command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`-f | --force`

Ignore non-existent Account Status Notification Handlers.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default null: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default null: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

3 Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has

been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-alert-handler

dsconfig delete-alert-handler — Deletes Alert Handlers

dsconfig delete-alert-handler

```
dsconfig delete-alert-handler {options}
```

1 Description

Deletes Alert Handlers.

2 Options

The **dsconfig delete-alert-handler** command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {name}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {name}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`-f | --force`

Ignore non-existent Alert Handlers.

Alert Handler properties depend on the Alert Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default null: JMX Alert Handler

Enabled by default: true

See the section called "JMX Alert Handler" for the properties of this Alert Handler type.

smtp-alert-handler

Default null: SMTP Alert Handler

Enabled by default: true

See the section called "SMTP Alert Handler" for the properties of this Alert Handler type.

3 JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-backend

dsconfig delete-backend — Deletes Backends

dsconfig delete-backend

```
dsconfig delete-backend {options}
```

1 Description

Deletes Backends.

2 Options

The **dsconfig delete-backend** command takes the following options:

`--backend-name {name}`

The name of the Backend.

Backend properties depend on the Backend type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {name}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {name}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {name}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {name}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {name}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {name}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {name}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {name}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {name}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {name}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {name}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`-f | --force`

Ignore non-existent Backends.

Backend properties depend on the Backend type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default null: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default null: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default null: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default null: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default null: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default null: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default null: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default null: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default null: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default null: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default null: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

3 Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

5 JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an

algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be

used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes

that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk

is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to

the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

10 PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE

(which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-backend-index

dsconfig delete-backend-index — Deletes Backend Indexes

dsconfig delete-backend-index

```
dsconfig delete-backend-index {options}
```

1 Description

Deletes Backend Indexes.

2 Options

The **dsconfig delete-backend-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--index-name {name}`

The name of the Backend Index.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`-f | --force`

Ignore non-existent Backend Indexes.

Backend Index properties depend on the Backend Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default null: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

3 Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-backend-vlv-index

dsconfig delete-backend-vlv-index — Deletes Backend VLV Indexes

dsconfig delete-backend-vlv-index

`dsconfig delete-backend-vlv-index` {options}

1 Description

Deletes Backend VLV Indexes.

2 Options

The **dsconfig delete-backend-vlv-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--index-name {name}`

The name of the Backend VLV Index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`-f | --force`

Ignore non-existent Backend VLV Indexes.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default null: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

3 Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

The VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig delete-certificate-mapper

dsconfig delete-certificate-mapper — Deletes Certificate Mappers

dsconfig delete-certificate-mapper

```
dsconfig delete-certificate-mapper {options}
```

1 Description

Deletes Certificate Mappers.

2 Options

The **dsconfig delete-certificate-mapper** command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`-f | --force`

Ignore non-existent Certificate Mappers.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default null: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default null: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default null: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default null: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

3 Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-connection-handler

dsconfig delete-connection-handler — Deletes Connection Handlers

dsconfig delete-connection-handler

```
dsconfig delete-connection-handler {options}
```

1 Description

Deletes Connection Handlers.

2 Options

The **dsconfig delete-connection-handler** command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {name}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {name}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {name}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {name}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {name}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`-f | --force`

Ignore non-existent Connection Handlers.

Connection Handler properties depend on the Connection Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default null: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default null: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default null: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default null: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default null: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

3 HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection

matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

5 LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended

response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection

matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig delete-debug-target

dsconfig delete-debug-target — Deletes Debug Targets

dsconfig delete-debug-target

```
dsconfig delete-debug-target {options}
```

1 Description

Deletes Debug Targets.

2 Options

The **dsconfig delete-debug-target** command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--target-name {name}`

The name of the Debug Target.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`-f | --force`

Ignore non-existent Debug Targets.

Debug Target properties depend on the Debug Target type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default null: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

3 Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-entry-cache

dsconfig delete-entry-cache — Deletes Entry Caches

dsconfig delete-entry-cache

```
dsconfig delete-entry-cache {options}
```

1 Description

Deletes Entry Caches.

2 Options

The **dsconfig delete-entry-cache** command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {name}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`-f | --force`

Ignore non-existent Entry Caches.

Entry Cache properties depend on the Entry Cache type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default null: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default null: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

3 FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-extended-operation-handler

dsconfig delete-extended-operation-handler — Deletes Extended Operation Handlers

dsconfig delete-extended-operation-handler

```
dsconfig delete-extended-operation-handler {options}
```

1 Description

Deletes Extended Operation Handlers.

2 Options

The **dsconfig delete-extended-operation-handler** command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`-f | --force`

Ignore non-existent Extended Operation Handlers.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default null: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default null: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default null: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default null: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default null: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default null: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default null: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

3 Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-group-implementation

dsconfig delete-group-implementation — Deletes Group Implementations

dsconfig delete-group-implementation

```
dsconfig delete-group-implementation {options}
```

1 Description

Deletes Group Implementations.

2 Options

The **dsconfig delete-group-implementation** command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {name}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {name}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`-f | --force`

Ignore non-existent Group Implementations.

Group Implementation properties depend on the Group Implementation type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default null: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default null: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default null: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

3 Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-http-authorization-mechanism

dsconfig delete-http-authorization-mechanism — Deletes HTTP Authorization Mechanisms

dsconfig delete-http-authorization-mechanism

```
dsconfig delete-http-authorization-mechanism {options}
```

1 Description

Deletes HTTP Authorization Mechanisms.

2 Options

The **dsconfig delete-http-authorization-mechanism** command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`-f | --force`

Ignore non-existent HTTP Authorization Mechanisms.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default null: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default null: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default null: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default null: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default null: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default null: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

3 HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

8 HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationM

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig delete-http-endpoint

dsconfig delete-http-endpoint — Deletes HTTP Endpoints

dsconfig delete-http-endpoint

```
dsconfig delete-http-endpoint {options}
```

1 Description

Deletes HTTP Endpoints.

2 Options

The **dsconfig delete-http-endpoint** command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {name}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {name}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`-f | --force`

Ignore non-existent HTTP Endpoints.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default null: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default null: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

3 Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-identity-mapper

dsconfig delete-identity-mapper — Deletes Identity Mappers

dsconfig delete-identity-mapper

```
dsconfig delete-identity-mapper {options}
```

1 Description

Deletes Identity Mappers.

2 Options

The **dsconfig delete-identity-mapper** command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`-f | --force`

Ignore non-existent Identity Mappers.

Identity Mapper properties depend on the Identity Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default null: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default null: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

3 Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-key-manager-provider

dsconfig delete-key-manager-provider — Deletes Key Manager Providers

dsconfig delete-key-manager-provider

```
dsconfig delete-key-manager-provider {options}
```

1 Description

Deletes Key Manager Providers.

2 Options

The **dsconfig delete-key-manager-provider** command takes the following options:

`--provider-name {name}`

The name of the Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {name}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`-f | --force`

Ignore non-existent Key Manager Providers.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default null: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default null: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default null: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

3 File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

5 PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig delete-log-publisher

dsconfig delete-log-publisher — Deletes Log Publishers

dsconfig delete-log-publisher

```
dsconfig delete-log-publisher {options}
```

1 Description

Deletes Log Publishers.

2 Options

The **dsconfig delete-log-publisher** command takes the following options:

`--publisher-name {name}`

The name of the Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {name}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {name}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {name}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {name}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`-f | --force`

Ignore non-existent Log Publishers.

Log Publisher properties depend on the Log Publisher type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default null: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default null: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default null: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default null: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default null: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default null: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default null: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default null: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default null: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default null: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default null: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

3 Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ

instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error

warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control,

admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

11 File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true OpenDJ

supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

12 Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-log-retention-policy

dsconfig delete-log-retention-policy — Deletes Log Retention Policies

dsconfig delete-log-retention-policy

```
dsconfig delete-log-retention-policy {options}
```

1 Description

Deletes Log Retention Policies.

2 Options

The **dsconfig delete-log-retention-policy** command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {name}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`-f | --force`

Ignore non-existent Log Retention Policies.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default null: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default null: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default null: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

3 File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-log-rotation-policy

dsconfig delete-log-rotation-policy — Deletes Log Rotation Policies

dsconfig delete-log-rotation-policy

```
dsconfig delete-log-rotation-policy {options}
```

1 Description

Deletes Log Rotation Policies.

2 Options

The **dsconfig delete-log-rotation-policy** command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`-f | --force`

Ignore non-existent Log Rotation Policies.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default null: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default null: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default null: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

3 Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-monitor-provider

dsconfig delete-monitor-provider — Deletes Monitor Providers

dsconfig delete-monitor-provider

```
dsconfig delete-monitor-provider {options}
```

1 Description

Deletes Monitor Providers.

2 Options

The **dsconfig delete-monitor-provider** command takes the following options:

`--provider-name {name}`

The name of the Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {name}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {name}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`-f | --force`

Ignore non-existent Monitor Providers.

Monitor Provider properties depend on the Monitor Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default null: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default null: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default null: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default null: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default null: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default null: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

3 Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-password-generator

dsconfig delete-password-generator — Deletes Password Generators

dsconfig delete-password-generator

```
dsconfig delete-password-generator {options}
```

1 Description

Deletes Password Generators.

2 Options

The **dsconfig delete-password-generator** command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {name}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`-f | --force`

Ignore non-existent Password Generators.

Password Generator properties depend on the Password Generator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default null: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

3 Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-password-policy

dsconfig delete-password-policy — Deletes Authentication Policies

dsconfig delete-password-policy

```
dsconfig delete-password-policy {options}
```

1 Description

Deletes Authentication Policies.

2 Options

The **dsconfig delete-password-policy** command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {name}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`-f | --force`

Ignore non-existent Authentication Policies.

Authentication Policy properties depend on the Authentication Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default null: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default null: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

3 LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- `w`: weeks

  Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP

servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially

waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This

attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed

password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse

previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times

in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-password-storage-scheme

dsconfig delete-password-storage-scheme — Deletes Password Storage Schemes

dsconfig delete-password-storage-scheme

```
dsconfig delete-password-storage-scheme {options}
```

1 Description

Deletes Password Storage Schemes.

2 Options

The **dsconfig delete-password-storage-scheme** command takes the following options:

`--scheme-name {name}`

The name of the Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {name}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`-f | --force`

Ignore non-existent Password Storage Schemes.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default null: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default null: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default null: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default null: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default null: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default null: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default null: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default null: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default null: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default null: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default null: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default null: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default null: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default null: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default null: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default null: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default null: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default null: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

3 AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

15 Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

16 Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

17 Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

18 Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

19 SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

20 Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-password-validator

dsconfig delete-password-validator — Deletes Password Validators

dsconfig delete-password-validator

```
dsconfig delete-password-validator {options}
```

1 Description

Deletes Password Validators.

2 Options

The **dsconfig delete-password-validator** command takes the following options:

`--validator-name {name}`

The name of the Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {name}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {name}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {name}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {name}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {name}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {name}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`-f | --force`

Ignore non-existent Password Validators.

Password Validator properties depend on the Password Validator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default null: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default null: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default null: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default null: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default null: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default null: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default null: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

3 Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges.

If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where

a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects

a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-plugin

dsconfig delete-plugin — Deletes Plugins

dsconfig delete-plugin

```
dsconfig delete-plugin {options}
```

1 Description

Deletes Plugins.

2 Options

The **dsconfig delete-plugin** command takes the following options:

`--plugin-name {name}`

The name of the Plugin.

Plugin properties depend on the Plugin type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {name}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {name}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {name}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {name}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {name}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {name}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {name}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {name}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {name}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`-f | --force`

Ignore non-existent Plugins.

Plugin properties depend on the Plugin type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default null: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default null: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default null: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default null: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default null: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default null: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default null: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default null: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default null: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default null: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default null: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default null: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

3 Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd

preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd

postOperationDelete

postOperationModify

postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

7 Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for

that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can

cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to

stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is

relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity

or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Changes to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

11 Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified,

and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete

postoperationmodifydn

subordinatemodifydn

subordinatedelete

preoperationadd

preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify

postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid

mail

userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preparseadd

preparsemodify

preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es):
org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

postoperationadd

postoperationmodify

postoperationmodifydn

postsynchronizationadd

postsynchronizationmodify

postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-replication-domain

dsconfig delete-replication-domain — Deletes Replication Domains

dsconfig delete-replication-domain

```
dsconfig delete-replication-domain {options}
```

1 Description

Deletes Replication Domains.

2 Options

The **dsconfig delete-replication-domain** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`-f | --force`

Ignore non-existent Replication Domains.

Replication Domain properties depend on the Replication Domain type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default null: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

3 Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval,

the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made

to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-replication-server

dsconfig delete-replication-server — Deletes Replication Servers

dsconfig delete-replication-server

```
dsconfig delete-replication-server {options}
```

1 Description

Deletes Replication Servers.

2 Options

The **dsconfig delete-replication-server** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {name}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`-f | --force`

Ignore non-existent Replication Servers.

Replication Server properties depend on the Replication Server type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default null: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

3 Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database.

Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-sasl-mechanism-handler

dsconfig delete-sasl-mechanism-handler — Deletes SASL Mechanism Handlers

dsconfig delete-sasl-mechanism-handler

```
dsconfig delete-sasl-mechanism-handler {options}
```

1 Description

Deletes SASL Mechanism Handlers.

2 Options

The **dsconfig delete-sasl-mechanism-handler** command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`-f | --force`

Ignore non-existent SASL Mechanism Handlers.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default null: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default null: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default null: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default null: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default null: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default null: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

3 Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided,

then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-schema-provider

dsconfig delete-schema-provider — Deletes Schema Providers

dsconfig delete-schema-provider

```
dsconfig delete-schema-provider {options}
```

1 Description

Deletes Schema Providers.

2 Options

The **dsconfig delete-schema-provider** command takes the following options:

`--provider-name {name}`

The name of the Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {name}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {name}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`-f | --force`

Ignore non-existent Schema Providers.

Schema Provider properties depend on the Schema Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default null: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default null: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

3 Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '*' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig delete-service-discovery-mechanism

dsconfig delete-service-discovery-mechanism — Deletes Service Discovery Mechanisms

dsconfig delete-service-discovery-mechanism

```
dsconfig delete-service-discovery-mechanism {options}
```

1 Description

Deletes Service Discovery Mechanisms.

2 Options

The **dsconfig delete-service-discovery-mechanism** command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`-f | --force`

Ignore non-existent Service Discovery Mechanisms.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default null: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default null: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

3 Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

4 Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig delete-synchronization-provider

dsconfig delete-synchronization-provider — Deletes Synchronization Providers

dsconfig delete-synchronization-provider

```
dsconfig delete-synchronization-provider {options}
```

1 Description

Deletes Synchronization Providers.

2 Options

The **dsconfig delete-synchronization-provider** command takes the following options:

`--provider-name {name}`

The name of the Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {name}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`-f | --force`

Ignore non-existent Synchronization Providers.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default null: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

3 Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig delete-trust-manager-provider

dsconfig delete-trust-manager-provider — Deletes Trust Manager Providers

dsconfig delete-trust-manager-provider

```
dsconfig delete-trust-manager-provider {options}
```

1 Description

Deletes Trust Manager Providers.

2 Options

The **dsconfig delete-trust-manager-provider** command takes the following options:

```
--provider-name {name}
```

The name of the Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`-f | --force`

Ignore non-existent Trust Manager Providers.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default null: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default null: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default null: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default null: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

3 Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

6 PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig delete-virtual-attribute

dsconfig delete-virtual-attribute — Deletes Virtual Attributes

dsconfig delete-virtual-attribute

```
dsconfig delete-virtual-attribute {options}
```

1 Description

Deletes Virtual Attributes.

2 Options

The **dsconfig delete-virtual-attribute** command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {name}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`-f | --force`

Ignore non-existent Virtual Attributes.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default null: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default null: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default null: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default null: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default null: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default null: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default null: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default null: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default null: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default null: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default null: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default null: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default null: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default null: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

3 Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

10 Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

14 Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

15 Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

16 User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-access-control-handler-prop

dsconfig get-access-control-handler-prop — Shows Access Control Handler properties

dsconfig get-access-control-handler-prop

```
dsconfig get-access-control-handler-prop {options}
```

1 Description

Shows Access Control Handler properties.

2 Options

The **dsconfig get-access-control-handler-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Access Control Handler properties depend on the Access Control Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

dsee-compat-access-control-handler

Default {property}: Dsee Compat Access Control Handler

Enabled by default: true

See the section called “Dsee Compat Access Control Handler” for the properties of this Access Control Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

dsee-compat-access-control-handler

Default null: Dsee Compat Access Control Handler

Enabled by default: true

See the section called “Dsee Compat Access Control Handler” for the properties of this Access Control Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Access Control Handler properties depend on the Access Control Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

dsee-compat-access-control-handler

Default {unit}: Dsee Compat Access Control Handler

Enabled by default: true

See the section called “Dsee Compat Access Control Handler” for the properties of this Access Control Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Access Control Handler properties depend on the Access Control Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Control Handler types:

dsee-compat-access-control-handler

Default {unit}: Dsee Compat Access Control Handler

Enabled by default: true

See the section called “Dsee Compat Access Control Handler” for the properties of this Access Control Handler type.

3 Dsee Compat Access Control Handler

Access Control Handlers of type dsee-compat-access-control-handler have the following properties:

enabled

Description

Indicates whether the Access Control Handler is enabled. If set to FALSE, then no access control is enforced, and any client (including unauthenticated or anonymous clients) could be allowed to perform any operation if not subject to other restrictions, such as those enforced by the privilege subsystem.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

global-aci

Description

Defines global access control rules. Global access control rules apply to all entries anywhere in the data managed by the OpenDJ directory server.

The global access control rules may be overridden by more specific access control rules placed in the data.

Default Value

No global access control rules are defined, which means that no access is allowed for any data in the server unless specifically granted by access control rules in the data.

Allowed Values

Section 5.1, “About Access Control Instructions”

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dsee Compat Access Control Handler implementation.

Default Value

org.opends.server.authorization.dseecompat.AciHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccessControlHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Access Control Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-access-log-filtering-criteria-prop

dsconfig get-access-log-filtering-criteria-prop — Shows Access Log Filtering Criteria properties

dsconfig get-access-log-filtering-criteria-prop

```
dsconfig get-access-log-filtering-criteria-prop {options}
```

1 Description

Shows Access Log Filtering Criteria properties.

2 Options

The **dsconfig get-access-log-filtering-criteria-prop** command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--property {property}`

The name of a property to be displayed.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {property}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`-E | --record`

Modifies the display output to show one property value per line.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default null: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

3 Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid

DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to

only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero

or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-account-status-notification-handler-prop

dsconfig get-account-status-notification-handler-prop — Shows Account Status Notification Handler properties

dsconfig get-account-status-notification-handler-prop

```
dsconfig get-account-status-notification-handler-prop {options}
```

1 Description

Shows Account Status Notification Handler properties.

2 Options

The **dsconfig get-account-status-notification-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`--property {property}`

The name of a property to be displayed.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {property}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {property}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default null: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default null: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

3 Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property

should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-administration-connector-prop

dsconfig get-administration-connector-prop — Shows Administration Connector properties

dsconfig get-administration-connector-prop

```
dsconfig get-administration-connector-prop {options}
```

1 Description

Shows Administration Connector properties.

2 Options

The **dsconfig get-administration-connector-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Administration Connector properties depend on the Administration Connector type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

administration-connector

Default {property}: Administration Connector

Enabled by default: false

See the section called “Administration Connector” for the properties of this Administration Connector type.

`-E | --record`

Modifies the display output to show one property value per line.

Administration Connector properties depend on the Administration Connector type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

administration-connector

Default null: Administration Connector

Enabled by default: false

See the section called “Administration Connector” for the properties of this Administration Connector type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Administration Connector properties depend on the Administration Connector type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

administration-connector

Default {unit}: Administration Connector

Enabled by default: false

See the section called “Administration Connector” for the properties of this Administration Connector type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Administration Connector properties depend on the Administration Connector type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Administration Connector types:

administration-connector

Default {unit}: Administration Connector

Enabled by default: false

See the section called “Administration Connector” for the properties of this Administration Connector type.

3 Administration Connector

Administration Connectors of type administration-connector have the following properties:

key-manager-provider

Description

Specifies the name of the key manager that is used with the Administration Connector .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this Administration Connector should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the Administration Connector listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the Administration Connector will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Administration Connector must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Administration Connector should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that is used with the Administration Connector .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

dsconfig get-alert-handler-prop

dsconfig get-alert-handler-prop — Shows Alert Handler properties

dsconfig get-alert-handler-prop

```
dsconfig get-alert-handler-prop {options}
```

1 Description

Shows Alert Handler properties.

2 Options

The **dsconfig get-alert-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {name}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {name}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`--property {property}`

The name of a property to be displayed.

Alert Handler properties depend on the Alert Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {property}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {property}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Alert Handler properties depend on the Alert Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default null: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default null: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {unit}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {unit}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {unit}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {unit}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

3 JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in

the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-backend-index-prop

dsconfig get-backend-index-prop — Shows Backend Index properties

dsconfig get-backend-index-prop

```
dsconfig get-backend-index-prop {options}
```

1 Description

Shows Backend Index properties.

2 Options

The **dsconfig get-backend-index-prop** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--index-name {name}`

The name of the Backend Index.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--property {property}`

The name of a property to be displayed.

Backend Index properties depend on the Backend Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {property}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`-E | --record`

Modifies the display output to show one property value per line.

Backend Index properties depend on the Backend Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default null: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {unit}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {unit}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

3 Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-backend-prop

dsconfig get-backend-prop — Shows Backend properties

dsconfig get-backend-prop

```
dsconfig get-backend-prop {options}
```

1 Description

Shows Backend properties.

2 Options

The **dsconfig get-backend-prop** command takes the following options:

`--backend-name {name}`

The name of the Backend.

Backend properties depend on the Backend type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {name}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {name}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {name}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {name}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {name}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {name}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {name}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {name}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {name}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {name}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {name}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`--property {property}`

The name of a property to be displayed.

Backend properties depend on the Backend type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {property}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {property}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {property}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {property}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {property}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {property}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {property}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {property}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {property}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {property}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {property}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`-E | --record`

Modifies the display output to show one property value per line.

Backend properties depend on the Backend type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default null: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default null: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default null: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default null: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default null: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default null: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default null: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default null: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default null: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default null: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default null: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {unit}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {unit}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {unit}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {unit}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {unit}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {unit}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {unit}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {unit}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {unit}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {unit}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {unit}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {unit}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {unit}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {unit}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {unit}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {unit}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {unit}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {unit}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {unit}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {unit}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {unit}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {unit}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

3 Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for

which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the

backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

5 JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise,

the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this

backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further

information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a

base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a

base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a

base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

10 PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two

backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that

should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- `w`: weeks

  Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the

value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE

(which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-backend-vlv-index-prop

dsconfig get-backend-vlv-index-prop — Shows Backend VLV Index properties

dsconfig get-backend-vlv-index-prop

```
dsconfig get-backend-vlv-index-prop {options}
```

1 Description

Shows Backend VLV Index properties.

2 Options

The **dsconfig get-backend-vlv-index-prop** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--index-name {name}`

The name of the Backend VLV Index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--property {property}`

The name of a property to be displayed.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {property}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`-E | --record`

Modifies the display output to show one property value per line.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default null: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {unit}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {unit}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

3 Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

The VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig get-certificate-mapper-prop

dsconfig get-certificate-mapper-prop — Shows Certificate Mapper properties

dsconfig get-certificate-mapper-prop

```
dsconfig get-certificate-mapper-prop {options}
```

1 Description

Shows Certificate Mapper properties.

2 Options

The **dsconfig get-certificate-mapper-prop** command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`--property {property}`

The name of a property to be displayed.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {property}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {property}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {property}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {property}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`-E | --record`

Modifies the display output to show one property value per line.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default null: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default null: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default null: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default null: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

3 Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-connection-handler-prop

dsconfig get-connection-handler-prop — Shows Connection Handler properties

dsconfig get-connection-handler-prop

```
dsconfig get-connection-handler-prop {options}
```

1 Description

Shows Connection Handler properties.

2 Options

The **dsconfig get-connection-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {name}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {name}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {name}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {name}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {name}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`--property {property}`

The name of a property to be displayed.

Connection Handler properties depend on the Connection Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {property}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {property}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {property}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {property}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {property}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Connection Handler properties depend on the Connection Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default null: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default null: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default null: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default null: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default null: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {unit}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {unit}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {unit}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {unit}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {unit}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {unit}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {unit}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {unit}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {unit}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {unit}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

3 HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts

rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple

addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept

new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

5 LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure

channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message

may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig get-crypto-manager-prop

dsconfig get-crypto-manager-prop — Shows Crypto Manager properties

dsconfig get-crypto-manager-prop

```
dsconfig get-crypto-manager-prop {options}
```

1 Description

Shows Crypto Manager properties.

2 Options

The **dsconfig get-crypto-manager-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Crypto Manager properties depend on the Crypto Manager type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

crypto-manager

Default {property}: Crypto Manager

Enabled by default: false

See the section called “Crypto Manager” for the properties of this Crypto Manager type.

`-E | --record`

Modifies the display output to show one property value per line.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

crypto-manager

Default null: Crypto Manager

Enabled by default: false

See the section called “Crypto Manager” for the properties of this Crypto Manager type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Crypto Manager properties depend on the Crypto Manager type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

crypto-manager

Default {unit}: Crypto Manager

Enabled by default: false

See the section called “Crypto Manager” for the properties of this Crypto Manager type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Crypto Manager properties depend on the Crypto Manager type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Crypto Manager types:

crypto-manager

Default {unit}: Crypto Manager

Enabled by default: false

See the section called “Crypto Manager” for the properties of this Crypto Manager type.

3 Crypto Manager

Crypto Managers of type crypto-manager have the following properties:

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server using the syntax algorithm/mode/padding. The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

digest-algorithm

Description

Specifies the preferred message digest algorithm for the directory server.

Default Value

SHA-256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately and only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-wrapping-transformation

Description

The preferred key wrapping transformation for the directory server. This value must be the same for all server instances in a replication topology.

Default Value

RSA/ECB/OAEPWITHSHA-1ANDMGF1PADDING

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect immediately but will only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

mac-algorithm

Description

Specifies the preferred MAC algorithm for the directory server.

Default Value

HmacSHA256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mac-key-length

Description

Specifies the key length in bits for the preferred MAC algorithm.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Crypto Manager should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Crypto Manager is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Crypto Manager must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-encryption

Description

Specifies whether SSL/TLS is used to provide encrypted communication between two OpenDJ server components.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

dsconfig get-debug-target-prop

dsconfig get-debug-target-prop — Shows Debug Target properties

dsconfig get-debug-target-prop

```
dsconfig get-debug-target-prop {options}
```

1 Description

Shows Debug Target properties.

2 Options

The **dsconfig get-debug-target-prop** command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--target-name {name}`

The name of the Debug Target.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--property {property}`

The name of a property to be displayed.

Debug Target properties depend on the Debug Target type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {property}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`-E | --record`

Modifies the display output to show one property value per line.

Debug Target properties depend on the Debug Target type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default null: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {unit}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {unit}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

3 Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-entry-cache-prop

dsconfig get-entry-cache-prop — Shows Entry Cache properties

dsconfig get-entry-cache-prop

```
dsconfig get-entry-cache-prop {options}
```

1 Description

Shows Entry Cache properties.

2 Options

The **dsconfig get-entry-cache-prop** command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {name}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`--property {property}`

The name of a property to be displayed.

Entry Cache properties depend on the Entry Cache type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {property}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {property}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`-E | --record`

Modifies the display output to show one property value per line.

Entry Cache properties depend on the Entry Cache type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default null: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default null: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {unit}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {unit}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

3 FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-extended-operation-handler-prop

dsconfig get-extended-operation-handler-prop — Shows Extended Operation Handler properties

dsconfig get-extended-operation-handler-prop

```
dsconfig get-extended-operation-handler-prop {options}
```

1 Description

Shows Extended Operation Handler properties.

2 Options

The **dsconfig get-extended-operation-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`--property {property}`

The name of a property to be displayed.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {property}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {property}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {property}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {property}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {property}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {property}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {property}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default null: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default null: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default null: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default null: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default null: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default null: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default null: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

3 Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-external-changelog-domain-prop

dsconfig get-external-changelog-domain-prop — Shows External Changelog Domain properties

dsconfig get-external-changelog-domain-prop

```
dsconfig get-external-changelog-domain-prop {options}
```

1 Description

Shows External Changelog Domain properties.

2 Options

The **dsconfig get-external-changelog-domain-prop** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {name}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`--domain-name {name}`

The name of the Replication Domain.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {name}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`--property {property}`

The name of a property to be displayed.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {property}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`-E | --record`

Modifies the display output to show one property value per line.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the null you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default null: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {unit}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {unit}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

3 External Changelog Domain

External Changelog Domains of type external-changelog-domain have the following properties:

ecl-include

Description

Specifies a list of attributes which should be published with every change log entry, regardless of whether the attribute itself has changed. The list of attributes may include wild cards such as "*" and "+" as well as object class references prefixed with an ampersand, for example "@person". The included attributes will be published using the "includedAttributes"

operational attribute as a single LDIF value rather like the "changes" attribute. For modify and modifyDN operations the included attributes will be taken from the entry before any changes were applied.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ecl-include-for-deletes

Description

Specifies a list of attributes which should be published with every delete operation change log entry, in addition to those specified by the "ecl-include" property. This property provides a means for applications to archive entries after they have been deleted. See the description of the "ecl-include" property for further information about how the included attributes are published.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the External Changelog Domain is enabled. To enable computing the change numbers, set the Replication Server's "ds-cfg-compute-change-number" property to true.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-global-configuration-prop

dsconfig get-global-configuration-prop — Shows Global Configuration properties

dsconfig get-global-configuration-prop

```
dsconfig get-global-configuration-prop {options}
```

1 Description

Shows Global Configuration properties.

2 Options

The **dsconfig get-global-configuration-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Global Configuration properties depend on the Global Configuration type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

global

Default {property}: Global Configuration

Enabled by default: false

See the section called “Global Configuration” for the properties of this Global Configuration type.

`-E | --record`

Modifies the display output to show one property value per line.

Global Configuration properties depend on the Global Configuration type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

global

Default null: Global Configuration

Enabled by default: false

See the section called “Global Configuration” for the properties of this Global Configuration type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Global Configuration properties depend on the Global Configuration type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

global

Default {unit}: Global Configuration

Enabled by default: false

See the section called “Global Configuration” for the properties of this Global Configuration type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Global Configuration properties depend on the Global Configuration type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Global Configuration types:

global

Default {unit}: Global Configuration

Enabled by default: false

See the section called “Global Configuration” for the properties of this Global Configuration type.

3 Global Configuration

Global Configurations of type global have the following properties:

add-missing-rdn-attributes

Description

Indicates whether the directory server should automatically add any attribute values contained in the entry's RDN into that entry when processing an add request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-attribute-name-exceptions

Description

Indicates whether the directory server should allow underscores in attribute names and allow attribute names to begin with numeric digits (both of which are violations of the LDAP standards).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-task

Description

Specifies the fully-qualified name of a Java class that may be invoked in the server. Any attempt to invoke a task not included in the list of allowed tasks is rejected.

Default Value

If no values are defined, then the server does not allow any tasks to be invoked.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

bind-with-dn-requires-password

Description

Indicates whether the directory server should reject any simple bind request that contains a DN but no password. Although such bind requests are technically allowed by the LDAPv3 specification (and should be treated as anonymous simple authentication), they may introduce security problems in applications that do not verify that the client actually provided a password.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-schema

Description

Indicates whether schema enforcement is active. When schema enforcement is activated, the directory server ensures that all operations result in entries are valid according to the defined server schema. It is strongly recommended that this option be left enabled to prevent the inadvertent addition of invalid data into the server.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-password-policy

Description

Specifies the name of the password policy that is in effect for users whose entries do not specify an alternate password policy (either via a real or virtual attribute). In addition, the default password policy will be used for providing default parameters for sub-entry based password policies when not provided or supported by the sub-entry itself. This property must reference a password policy and no other type of authentication policy.

Default Value

None

Allowed Values

The DN of any Password Policy.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-privilege

Description

Specifies the name of a privilege that should not be evaluated by the server. If a privilege is disabled, then it is assumed that all clients (including unauthenticated clients) have that privilege.

Default Value

If no values are defined, then the server enforces all privileges.

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

The privilege that provides the ability to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

etime-resolution

Description

Specifies the resolution to use for operation elapsed processing time (etime) measurements.

Default Value

milliseconds

Allowed Values

milliseconds

Use millisecond resolution.

nanoseconds

Use nanosecond resolution.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-time-limit

Description

Specifies the maximum length of time that a client connection may remain established since its last completed operation. A value of "0 seconds" indicates that no idle time limit is enforced.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

invalid-attribute-syntax-behavior

Description

Specifies how the directory server should handle operations whenever an attribute value violates the associated attribute syntax.

Default Value

reject

Allowed Values

accept

The directory server silently accepts attribute values that are invalid according to their associated syntax. Matching operations targeting those values may not behave as expected.

reject

The directory server rejects attribute values that are invalid according to their associated syntax.

warn

The directory server accepts attribute values that are invalid according to their associated syntax, but also logs a warning message to the error log. Matching operations targeting those values may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lookthrough-limit

Description

Specifies the maximum number of entries that the directory server should "look through" in the course of processing a search request. This includes any entry that the server must examine in the course of processing the request, regardless of whether it actually matches the search criteria. A value of 0 indicates that no lookthrough limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-lookthrough-limit operational attribute.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-allowed-client-connections

Description

Specifies the maximum number of client connections that may be established at any given time A value of 0 indicates that unlimited client connection is allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-internal-buffer-size

Description

The threshold capacity beyond which internal cached buffers used for encoding and decoding entries and protocol messages will be trimmed after use. Individual buffers may grow very large when encoding and decoding large entries and protocol messages and should be reduced in size when they are no longer needed. This setting specifies the threshold at which a buffer is determined to have grown too big and should be trimmed down after use.

Default Value

32 KB

Allowed Values

Lower value is 512.Upper value is 1000000000.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-psearches

Description

Defines the maximum number of concurrent persistent searches that can be performed on directory server The persistent search mechanism provides an active channel through which entries that change, and information about the changes that occur, can be communicated. Because each persistent search operation consumes resources, limiting the number of simultaneous persistent searches keeps the performance impact minimal. A value of -1 indicates that there is no limit on the persistent searches.

Default Value

-1

Allowed Values

An integer value. Lower value is 0. A value of "-1" or "unlimited" for no limit.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

notify-abandoned-operations

Description

Indicates whether the directory server should send a response to any operation that is interrupted via an abandon request. The LDAP specification states that abandoned operations should not receive any response, but this may cause problems with client applications that always expect to receive a response to each request.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

proxied-authorization-identity-mapper

Description

Specifies the name of the identity mapper to map authorization ID values (using the "u:" form) provided in the proxied authorization control to the corresponding user entry.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

reject-unauthenticated-requests

Description

Indicates whether the directory server should reject any request (other than bind or StartTLS requests) received from a client that has not yet been authenticated, whose last authentication attempt was unsuccessful, or whose last authentication attempt used anonymous authentication.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

return-bind-error-messages

Description

Indicates whether responses for failed bind operations should include a message string providing the reason for the authentication failure. Note that these messages may include information that could potentially be used by an attacker. If this option is disabled, then these messages appears only in the server's access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

save-config-on-successful-startup

Description

Indicates whether the directory server should save a copy of its configuration whenever the startup process completes successfully. This ensures that the server provides a "last known good" configuration, which can be used as a reference (or copied into the active config) if the server fails to start with the current "active" configuration.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-error-result-code

Description

Specifies the numeric value of the result code when request processing fails due to an internal server error.

Default Value

80

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

single-structural-objectclass-behavior

Description

Specifies how the directory server should handle operations an entry does not contain a structural object class or contains multiple structural classes.

Default Value

reject

Allowed Values

accept

The directory server silently accepts entries that do not contain exactly one structural object class. Certain schema features that depend on the entry's structural class may not behave as expected.

reject

The directory server rejects entries that do not contain exactly one structural object class.

warn

The directory server accepts entries that do not contain exactly one structural object class, but also logs a warning message to the error log. Certain schema features that depend on the entry's structural class may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

size-limit

Description

Specifies the maximum number of entries that can be returned to the client during a single search operation. A value of 0 indicates that no size

limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-size-limit operational attribute.

Default Value

1000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

smtp-server

Description

Specifies the address (and optional port number) for a mail server that can be used to send email messages via SMTP. It may be an IP address or resolvable hostname, optionally followed by a colon and a port number.

Default Value

If no values are defined, then the server cannot send email via SMTP.

Allowed Values

A hostname, optionally followed by a ":" followed by a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

subordinate-base-dn

Description

Specifies the set of base DNs used for singleLevel, wholeSubtree, and subordinateSubtree searches based at the root DSE.

Default Value

The set of all user-defined suffixes is used.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-limit

Description

Specifies the maximum length of time that should be spent processing a single search operation. A value of 0 seconds indicates that no time limit is enforced. Note that this is the default server-wide time limit, but it may be overridden on a per-user basis using the ds-rlim-time-limit operational attribute.

Default Value

60 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-transaction-ids

Description

Indicates whether the directory server should trust the transaction ids that may be received from requests, either through a LDAP control or through a HTTP header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the kinds of write operations the directory server can process.

Default Value

enabled

Allowed Values

disabled

The directory server rejects all write operations that are requested of it, regardless of their origin.

enabled

The directory server attempts to process all write operations that are requested of it, regardless of their origin.

internal-only

The directory server attempts to process write operations requested as internal operations or through synchronization, but rejects any such operations requested from external clients.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-group-implementation-prop

dsconfig get-group-implementation-prop — Shows Group Implementation properties

dsconfig get-group-implementation-prop

```
dsconfig get-group-implementation-prop {options}
```

1 Description

Shows Group Implementation properties.

2 Options

The **dsconfig get-group-implementation-prop** command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {name}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {name}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`--property {property}`

The name of a property to be displayed.

Group Implementation properties depend on the Group Implementation type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {property}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {property}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {property}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`-E | --record`

Modifies the display output to show one property value per line.

Group Implementation properties depend on the Group Implementation type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default null: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default null: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default null: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {unit}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {unit}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

3 Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-http-authorization-mechanism-prop

dsconfig get-http-authorization-mechanism-prop — Shows HTTP Authorization Mechanism properties

dsconfig get-http-authorization-mechanism-prop

`dsconfig get-http-authorization-mechanism-prop {options}`

1 Description

Shows HTTP Authorization Mechanism properties.

2 Options

The **dsconfig get-http-authorization-mechanism-prop** command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`--property {property}`

The name of a property to be displayed.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {property}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {property}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {property}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {property}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {property}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {property}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`-E | --record`

Modifies the display output to show one property value per line.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default null: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default null: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default null: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default null: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default null: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default null: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

3 HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

8 HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationM

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig get-http-endpoint-prop

dsconfig get-http-endpoint-prop — Shows HTTP Endpoint properties

dsconfig get-http-endpoint-prop

```
dsconfig get-http-endpoint-prop {options}
```

1 Description

Shows HTTP Endpoint properties.

2 Options

The **dsconfig get-http-endpoint-prop** command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {name}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {name}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`--property {property}`

The name of a property to be displayed.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {property}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {property}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`-E | --record`

Modifies the display output to show one property value per line.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the null you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default null: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default null: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {unit}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {unit}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

3 Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-identity-mapper-prop

dsconfig get-identity-mapper-prop — Shows Identity Mapper properties

dsconfig get-identity-mapper-prop

```
dsconfig get-identity-mapper-prop {options}
```

1 Description

Shows Identity Mapper properties.

2 Options

The **dsconfig get-identity-mapper-prop** command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`--property {property}`

The name of a property to be displayed.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {property}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {property}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`-E | --record`

Modifies the display output to show one property value per line.

Identity Mapper properties depend on the Identity Mapper type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default null: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default null: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

3 Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-key-manager-provider-prop

dsconfig get-key-manager-provider-prop — Shows Key Manager Provider properties

dsconfig get-key-manager-provider-prop

```
dsconfig get-key-manager-provider-prop {options}
```

1 Description

Shows Key Manager Provider properties.

2 Options

The **dsconfig get-key-manager-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {name}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`--property {property}`

The name of a property to be displayed.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {property}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {property}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {property}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default null: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default null: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default null: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

3 File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

5 PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig get-log-publisher-prop

dsconfig get-log-publisher-prop — Shows Log Publisher properties

dsconfig get-log-publisher-prop

```
dsconfig get-log-publisher-prop {options}
```

1 Description

Shows Log Publisher properties.

2 Options

The **dsconfig get-log-publisher-prop** command takes the following options:

`--publisher-name {name}`

The name of the Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {name}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {name}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {name}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {name}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`--property {property}`

The name of a property to be displayed.

Log Publisher properties depend on the Log Publisher type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {property}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {property}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {property}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {property}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {property}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {property}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {property}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {property}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {property}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {property}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {property}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`-E | --record`

Modifies the display output to show one property value per line.

Log Publisher properties depend on the Log Publisher type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default null: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default null: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default null: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default null: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default null: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default null: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default null: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default null: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default null: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default null: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default null: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {unit}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {unit}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

3 Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ

instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error

warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control,

admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

11 File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true OpenDJ

supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

12 Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-log-retention-policy-prop

dsconfig get-log-retention-policy-prop — Shows Log Retention Policy properties

dsconfig get-log-retention-policy-prop

```
dsconfig get-log-retention-policy-prop {options}
```

1 Description

Shows Log Retention Policy properties.

2 Options

The **dsconfig get-log-retention-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {name}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`--property {property}`

The name of a property to be displayed.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {property}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {property}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {property}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`-E | --record`

Modifies the display output to show one property value per line.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default null: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default null: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default null: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

3 File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-log-rotation-policy-prop

dsconfig get-log-rotation-policy-prop — Shows Log Rotation Policy properties

dsconfig get-log-rotation-policy-prop

```
dsconfig get-log-rotation-policy-prop {options}
```

1 Description

Shows Log Rotation Policy properties.

2 Options

The **dsconfig get-log-rotation-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`--property {property}`

The name of a property to be displayed.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {property}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {property}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {property}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`-E | --record`

Modifies the display output to show one property value per line.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default null: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default null: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default null: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

3 Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-monitor-provider-prop

dsconfig get-monitor-provider-prop — Shows Monitor Provider properties

dsconfig get-monitor-provider-prop

```
dsconfig get-monitor-provider-prop {options}
```

1 Description

Shows Monitor Provider properties.

2 Options

The **dsconfig get-monitor-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {name}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {name}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`--property {property}`

The name of a property to be displayed.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {property}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {property}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {property}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {property}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {property}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {property}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Monitor Provider properties depend on the Monitor Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default null: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default null: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default null: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default null: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default null: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default null: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {unit}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {unit}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {unit}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {unit}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

3 Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es):
org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-password-generator-prop

dsconfig get-password-generator-prop — Shows Password Generator properties

dsconfig get-password-generator-prop

```
dsconfig get-password-generator-prop {options}
```

1 Description

Shows Password Generator properties.

2 Options

The **dsconfig get-password-generator-prop** command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {name}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`--property {property}`

The name of a property to be displayed.

Password Generator properties depend on the Password Generator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {property}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`-E | --record`

Modifies the display output to show one property value per line.

Password Generator properties depend on the Password Generator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default null: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {unit}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {unit}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

3 Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-password-policy-prop

dsconfig get-password-policy-prop — Shows Authentication Policy properties

dsconfig get-password-policy-prop

```
dsconfig get-password-policy-prop {options}
```

1 Description

Shows Authentication Policy properties.

2 Options

The **dsconfig get-password-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {name}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`--property {property}`

The name of a property to be displayed.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {property}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {property}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`-E | --record`

Modifies the display output to show one property value per line.

Authentication Policy properties depend on the Authentication Policy type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default null: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default null: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {unit}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {unit}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

3 LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using

the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP

keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text

version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives.

If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed

by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- `w`: weeks

  Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind

responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity

or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-password-storage-scheme-prop

dsconfig get-password-storage-scheme-prop — Shows Password Storage Scheme properties

dsconfig get-password-storage-scheme-prop

```
dsconfig get-password-storage-scheme-prop {options}
```

1 Description

Shows Password Storage Scheme properties.

2 Options

The **dsconfig get-password-storage-scheme-prop** command takes the following options:

`--scheme-name {name}`

The name of the Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {name}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`--property {property}`

The name of a property to be displayed.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {property}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {property}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {property}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {property}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {property}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {property}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {property}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {property}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {property}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {property}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {property}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {property}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {property}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {property}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {property}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {property}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {property}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {property}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`-E | --record`

Modifies the display output to show one property value per line.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default null: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default null: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default null: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default null: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default null: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default null: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default null: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default null: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default null: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default null: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default null: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default null: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default null: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default null: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default null: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default null: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default null: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default null: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

3 AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

15 Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

16 Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

17 Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

18 Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

19 SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

20 Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-password-validator-prop

dsconfig get-password-validator-prop — Shows Password Validator properties

dsconfig get-password-validator-prop

```
dsconfig get-password-validator-prop {options}
```

1 Description

Shows Password Validator properties.

2 Options

The **dsconfig get-password-validator-prop** command takes the following options:

`--validator-name {name}`

The name of the Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {name}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {name}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {name}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {name}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {name}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {name}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`--property {property}`

The name of a property to be displayed.

Password Validator properties depend on the Password Validator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {property}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {property}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {property}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {property}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {property}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {property}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {property}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`-E | --record`

Modifies the display output to show one property value per line.

Password Validator properties depend on the Password Validator type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default null: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default null: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default null: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default null: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default null: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default null: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default null: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {unit}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {unit}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {unit}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {unit}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {unit}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {unit}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

3 Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are

provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating

the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-plugin-prop

dsconfig get-plugin-prop — Shows Plugin properties

dsconfig get-plugin-prop

```
dsconfig get-plugin-prop {options}
```

1 Description

Shows Plugin properties.

2 Options

The **dsconfig get-plugin-prop** command takes the following options:

`--plugin-name {name}`

The name of the Plugin.

Plugin properties depend on the Plugin type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {name}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {name}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {name}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {name}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {name}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {name}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {name}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {name}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {name}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`--property {property}`

The name of a property to be displayed.

Plugin properties depend on the Plugin type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {property}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {property}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {property}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {property}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {property}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {property}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {property}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {property}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {property}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {property}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {property}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {property}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`-E | --record`

Modifies the display output to show one property value per line.

Plugin properties depend on the Plugin type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default null: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default null: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default null: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default null: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default null: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default null: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default null: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default null: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default null: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default null: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default null: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default null: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {unit}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {unit}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {unit}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {unit}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {unit}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {unit}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {unit}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {unit}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {unit}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {unit}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

3 Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd

preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd

postOperationDelete

postOperationModify

postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

7 Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for

that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can

cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to

stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is

relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity

or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Changes to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

11 Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified,

and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete

postoperationmodifydn

subordinatemodifydn

subordinatedelete

preoperationadd

preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify

postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid

mail

userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preparseadd

preparsemodify

preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

postoperationadd

postoperationmodify

postoperationmodifydn

postsynchronizationadd

postsynchronizationmodify

postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-plugin-root-prop

dsconfig get-plugin-root-prop — Shows Plugin Root properties

dsconfig get-plugin-root-prop

```
dsconfig get-plugin-root-prop {options}
```

1 Description

Shows Plugin Root properties.

2 Options

The **dsconfig get-plugin-root-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Plugin Root properties depend on the Plugin Root type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Plugin Root types:

plugin-root

Default {property}: Plugin Root

Enabled by default: false

See the section called “Plugin Root” for the properties of this Plugin Root type.

`-E | --record`

Modifies the display output to show one property value per line.

Plugin Root properties depend on the Plugin Root type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Plugin Root types:

plugin-root

Default null: Plugin Root

Enabled by default: false

See the section called “Plugin Root” for the properties of this Plugin Root type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Plugin Root properties depend on the Plugin Root type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin Root types:

plugin-root

Default {unit}: Plugin Root

Enabled by default: false

See the section called “Plugin Root” for the properties of this Plugin Root type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Plugin Root properties depend on the Plugin Root type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin Root types:

plugin-root

Default {unit}: Plugin Root

Enabled by default: false

See the section called “Plugin Root” for the properties of this Plugin Root type.

3 Plugin Root

Plugin Roots of type plugin-root have the following properties:

plugin-order-intermediate-response

Description

Specifies the order in which intermediate response plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-

in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which intermediate response plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-export

Description

Specifies the order in which LDIF export plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF export plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import

Description

Specifies the order in which LDIF import plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-begin

Description

Specifies the order in which LDIF import begin plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import begin plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-end

Description

Specifies the order in which LDIF import end plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import end plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-connect

Description

Specifies the order in which post-connect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-connect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-disconnect

Description

Specifies the order in which post-disconnect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-disconnect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-abandon

Description

Specifies the order in which post-operation abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-add

Description

Specifies the order in which post-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-bind

Description

Specifies the order in which post-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where

the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-compare

Description

Specifies the order in which post-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-delete

Description

Specifies the order in which post-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-extended

Description

Specifies the order in which post-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify

Description

Specifies the order in which post-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify-dn

Description

Specifies the order in which post-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-search

Description

Specifies the order in which post-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-unbind

Description

Specifies the order in which post-operation unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-add

Description

Specifies the order in which post-response add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-bind

Description

Specifies the order in which post-response bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where

the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-compare

Description

Specifies the order in which post-response compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-delete

Description

Specifies the order in which post-response delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-extended

Description

Specifies the order in which post-response extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify

Description

Specifies the order in which post-response modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify-dn

Description

Specifies the order in which post-response modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-search

Description

Specifies the order in which post-response search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-add

Description

Specifies the order in which post-synchronization add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-delete

Description

Specifies the order in which post-synchronization delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify

Description

Specifies the order in which post-synchronization modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-

in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify-dn

Description

Specifies the order in which post-synchronization modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-add

Description

Specifies the order in which pre-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-bind

Description

Specifies the order in which pre-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-compare

Description

Specifies the order in which pre-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-delete

Description

Specifies the order in which pre-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-extended

Description

Specifies the order in which pre-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify

Description

Specifies the order in which pre-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify-dn

Description

Specifies the order in which pre-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-search

Description

Specifies the order in which pre-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names

(where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation searc plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-abandon

Description

Specifies the order in which pre-parse abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-add

Description

Specifies the order in which pre-parse add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-bind

Description

Specifies the order in which pre-parse bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-compare

Description

Specifies the order in which pre-parse compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-delete

Description

Specifies the order in which pre-parse delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-extended

Description

Specifies the order in which pre-parse extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify

Description

Specifies the order in which pre-parse modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify-dn

Description

Specifies the order in which pre-parse modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-search

Description

Specifies the order in which pre-parse search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where

the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-unbind

Description

Specifies the order in which pre-parse unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-entry

Description

Specifies the order in which search result entry plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result entry plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-reference

Description

Specifies the order in which search result reference plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result reference plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-shutdown

Description

Specifies the order in which shutdown plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which shutdown plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-startup

Description

Specifies the order in which startup plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which startup plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-delete

Description

Specifies the order in which subordinate delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-modify-dn

Description

Specifies the order in which subordinate modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-replication-domain-prop

dsconfig get-replication-domain-prop — Shows Replication Domain properties

dsconfig get-replication-domain-prop

`dsconfig get-replication-domain-prop {options}`

1 Description

Shows Replication Domain properties.

2 Options

The **dsconfig get-replication-domain-prop** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--property {property}`

The name of a property to be displayed.

Replication Domain properties depend on the Replication Domain type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {property}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`-E | --record`

Modifies the display output to show one property value per line.

Replication Domain properties depend on the Replication Domain type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default null: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {unit}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {unit}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

3 Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds

- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects

a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made

to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts. When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-replication-server-prop

dsconfig get-replication-server-prop — Shows Replication Server properties

dsconfig get-replication-server-prop

```
dsconfig get-replication-server-prop {options}
```

1 Description

Shows Replication Server properties.

2 Options

The **dsconfig get-replication-server-prop** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {name}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`--property {property}`

The name of a property to be displayed.

Replication Server properties depend on the Replication Server type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {property}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`-E | --record`

Modifies the display output to show one property value per line.

Replication Server properties depend on the Replication Server type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default null: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {unit}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {unit}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

3 Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- w: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality

is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status

analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- w: weeks

  Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different

power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-root-dn-prop

dsconfig get-root-dn-prop — Shows Root DN properties

dsconfig get-root-dn-prop

```
dsconfig get-root-dn-prop {options}
```

1 Description

Shows Root DN properties.

2 Options

The **dsconfig get-root-dn-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Root DN properties depend on the Root DN type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Root DN types:

root-dn

Default {property}: Root DN

Enabled by default: false

See the section called “Root DN” for the properties of this Root DN type.

`-E | --record`

Modifies the display output to show one property value per line.

Root DN properties depend on the Root DN type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Root DN types:

root-dn

Default null: Root DN

Enabled by default: false

See the section called “Root DN” for the properties of this Root DN type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Root DN properties depend on the Root DN type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DN types:

root-dn

Default {unit}: Root DN

Enabled by default: false

See the section called “Root DN” for the properties of this Root DN type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Root DN properties depend on the Root DN type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DN types:

root-dn

Default {unit}: Root DN

Enabled by default: false

See the section called “Root DN” for the properties of this Root DN type.

3 Root DN

Root Dns of type root-dn have the following properties:

default-root-privilege-name

Description

Specifies the names of the privileges that root users will be granted by default.

Default Value

bypass-lockdown

bypass-acl

modify-acl

config-read

config-write

ldif-import

ldif-export

backend-backup

backend-restore

server-lockdown

server-shutdown

server-restart

disconnect-client

cancel-request

password-reset

update-schema

privilege-change

unindexed-search

subentry-write

changelog-read

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

Allows the user to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-root-dse-backend-prop

dsconfig get-root-dse-backend-prop — Shows Root DSE Backend properties

dsconfig get-root-dse-backend-prop

```
dsconfig get-root-dse-backend-prop {options}
```

1 Description

Shows Root DSE Backend properties.

2 Options

The **dsconfig get-root-dse-backend-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Root DSE Backend types:

root-dse-backend

Default {property}: Root DSE Backend

Enabled by default: false

See the section called “Root DSE Backend” for the properties of this Root DSE Backend type.

`-E | --record`

Modifies the display output to show one property value per line.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Root DSE Backend types:

root-dse-backend

Default null: Root DSE Backend

Enabled by default: false

See the section called “Root DSE Backend” for the properties of this Root DSE Backend type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DSE Backend types:

root-dse-backend

Default {unit}: Root DSE Backend

Enabled by default: false

See the section called “Root DSE Backend” for the properties of this Root DSE Backend type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Root DSE Backend types:

root-dse-backend

Default {unit}: Root DSE Backend

Enabled by default: false

See the section called “Root DSE Backend” for the properties of this Root DSE Backend type.

3 Root DSE Backend

Root DSE Backends of type root-dse-backend have the following properties:

show-all-attributes

Description

Indicates whether all attributes in the root DSE are to be treated like user attributes (and therefore returned to clients by default) regardless of the directory server schema configuration.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

show-subordinate-naming-contexts

Description

Indicates whether subordinate naming contexts should be visible in the namingContexts attribute of the RootDSE. By default only top level naming contexts are visible

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-sasl-mechanism-handler-prop

dsconfig get-sasl-mechanism-handler-prop — Shows SASL Mechanism Handler properties

dsconfig get-sasl-mechanism-handler-prop

```
dsconfig get-sasl-mechanism-handler-prop {options}
```

1 Description

Shows SASL Mechanism Handler properties.

2 Options

The **dsconfig get-sasl-mechanism-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`--property {property}`

The name of a property to be displayed.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {property}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {property}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {property}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {property}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {property}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {property}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`-E | --record`

Modifies the display output to show one property value per line.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the null you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default null: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default null: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default null: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default null: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default null: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default null: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

3 Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-schema-provider-prop

dsconfig get-schema-provider-prop — Shows Schema Provider properties

dsconfig get-schema-provider-prop

```
dsconfig get-schema-provider-prop {options}
```

1 Description

Shows Schema Provider properties.

2 Options

The **dsconfig get-schema-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {name}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {name}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`--property {property}`

The name of a property to be displayed.

Schema Provider properties depend on the Schema Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {property}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {property}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Schema Provider properties depend on the Schema Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default null: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default null: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {unit}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {unit}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {unit}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {unit}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

3 Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '*' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-service-discovery-mechanism-prop

dsconfig get-service-discovery-mechanism-prop — Shows Service Discovery Mechanism properties

dsconfig get-service-discovery-mechanism-prop

`dsconfig get-service-discovery-mechanism-prop {options}`

1 Description

Shows Service Discovery Mechanism properties.

2 Options

The **dsconfig get-service-discovery-mechanism-prop** command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`--property {property}`

The name of a property to be displayed.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {property}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {property}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`-E | --record`

Modifies the display output to show one property value per line.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default null: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default null: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

3 Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private)

key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

4 Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig get-synchronization-provider-prop

dsconfig get-synchronization-provider-prop — Shows Synchronization Provider properties

dsconfig get-synchronization-provider-prop

```
dsconfig get-synchronization-provider-prop {options}
```

1 Description

Shows Synchronization Provider properties.

2 Options

The **dsconfig get-synchronization-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {name}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`--property {property}`

The name of a property to be displayed.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {property}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default null: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

3 Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- w: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig get-trust-manager-provider-prop

dsconfig get-trust-manager-provider-prop — Shows Trust Manager Provider properties

dsconfig get-trust-manager-provider-prop

```
dsconfig get-trust-manager-provider-prop {options}
```

1 Description

Shows Trust Manager Provider properties.

2 Options

The **dsconfig get-trust-manager-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`--property {property}`

The name of a property to be displayed.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {property}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {property}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {property}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {property}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`-E | --record`

Modifies the display output to show one property value per line.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default null: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default null: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default null: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default null: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

3 Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root.

Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

6 PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig get-virtual-attribute-prop

dsconfig get-virtual-attribute-prop — Shows Virtual Attribute properties

dsconfig get-virtual-attribute-prop

```
dsconfig get-virtual-attribute-prop {options}
```

1 Description

Shows Virtual Attribute properties.

2 Options

The **dsconfig get-virtual-attribute-prop** command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {name}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`--property {property}`

The name of a property to be displayed.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {property}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {property}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {property}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {property}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {property}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {property}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {property}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {property}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {property}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {property}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {property}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {property}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {property}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {property}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`-E | --record`

Modifies the display output to show one property value per line.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default null: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default null: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default null: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default null: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default null: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default null: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default null: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default null: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default null: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default null: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default null: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default null: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default null: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default null: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {unit}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {unit}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

3 Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

10 Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

14 Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

15 Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

16 User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig get-work-queue-prop

dsconfig get-work-queue-prop — Shows Work Queue properties

dsconfig get-work-queue-prop

```
dsconfig get-work-queue-prop {options}
```

1 Description

Shows Work Queue properties.

2 Options

The **dsconfig get-work-queue-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Work Queue properties depend on the Work Queue type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Work Queue types:

parallel-work-queue

Default {property}: Parallel Work Queue

Enabled by default: false

See the section called “Parallel Work Queue” for the properties of this Work Queue type.

traditional-work-queue

Default {property}: Traditional Work Queue

Enabled by default: false

See the section called “Traditional Work Queue” for the properties of this Work Queue type.

`-E | --record`

Modifies the display output to show one property value per line.

Work Queue properties depend on the Work Queue type, which depends on the null you provide.

By default, OpenDJ directory server supports the following Work Queue types:

parallel-work-queue

Default null: Parallel Work Queue

Enabled by default: false

See the section called “Parallel Work Queue” for the properties of this Work Queue type.

traditional-work-queue

Default null: Traditional Work Queue

Enabled by default: false

See the section called “Traditional Work Queue” for the properties of this Work Queue type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Work Queue properties depend on the Work Queue type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Work Queue types:

parallel-work-queue

Default {unit}: Parallel Work Queue

Enabled by default: false

See the section called “Parallel Work Queue” for the properties of this Work Queue type.

traditional-work-queue

Default {unit}: Traditional Work Queue

Enabled by default: false

See the section called “Traditional Work Queue” for the properties of this Work Queue type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Work Queue properties depend on the Work Queue type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Work Queue types:

parallel-work-queue

Default {unit}: Parallel Work Queue

Enabled by default: false

See the section called “Parallel Work Queue” for the properties of this Work Queue type.

traditional-work-queue

Default {unit}: Traditional Work Queue

Enabled by default: false

See the section called “Traditional Work Queue” for the properties of this Work Queue type.

3 Parallel Work Queue

Work Queues of type parallel-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Parallel Work Queue implementation.

Default Value

org.opends.server.extensions.ParallelWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Traditional Work Queue

Work Queues of type traditional-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Traditional Work Queue implementation.

Default Value

org.opends.server.extensions.TraditionalWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-work-queue-capacity

Description

Specifies the maximum number of queued operations that can be in the work queue at any given time. If the work queue is already full and

additional requests are received by the server, then the server front end, and possibly the client, will be blocked until the work queue has available capacity.

Default Value

1000

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-access-log-filtering-criteria

dsconfig list-access-log-filtering-criteria — Lists existing Access Log Filtering Criteria

dsconfig list-access-log-filtering-criteria

```
dsconfig list-access-log-filtering-criteria {options}
```

1 Description

Lists existing Access Log Filtering Criteria.

2 Options

The **dsconfig list-access-log-filtering-criteria** command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--property {property}`

The name of a property to be displayed.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {property}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {unit}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

3 Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-account-status-notification-handlers

dsconfig list-account-status-notification-handlers — Lists existing Account Status Notification Handlers

dsconfig list-account-status-notification-handlers

```
dsconfig list-account-status-notification-handlers {options}
```

1 Description

Lists existing Account Status Notification Handlers.

2 Options

The **dsconfig list-account-status-notification-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {property}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {property}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {unit}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {unit}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

3 Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only

applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-alert-handlers

dsconfig list-alert-handlers — Lists existing Alert Handlers

dsconfig list-alert-handlers

```
dsconfig list-alert-handlers {options}
```

1 Description

Lists existing Alert Handlers.

2 Options

The **dsconfig list-alert-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Alert Handler properties depend on the Alert Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {property}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {property}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {unit}: JMX Alert Handler

Enabled by default: true

See the section called "JMX Alert Handler" for the properties of this Alert Handler type.

smtp-alert-handler

Default {unit}: SMTP Alert Handler

Enabled by default: true

See the section called "SMTP Alert Handler" for the properties of this Alert Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Alert Handler properties depend on the Alert Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {unit}: JMX Alert Handler

Enabled by default: true

See the section called "JMX Alert Handler" for the properties of this Alert Handler type.

smtp-alert-handler

Default {unit}: SMTP Alert Handler

Enabled by default: true

See the section called "SMTP Alert Handler" for the properties of this Alert Handler type.

3 JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-backend-indexes

dsconfig list-backend-indexes — Lists existing Backend Indexes

dsconfig list-backend-indexes

```
dsconfig list-backend-indexes {options}
```

1 Description

Lists existing Backend Indexes.

2 Options

The **dsconfig list-backend-indexes** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--property {property}`

The name of a property to be displayed.

Backend Index properties depend on the Backend Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {property}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {unit}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend Index properties depend on the Backend Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {unit}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

3 Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-backend-vlv-indexes

dsconfig list-backend-vlv-indexes — Lists existing Backend VLV Indexes

dsconfig list-backend-vlv-indexes

`dsconfig list-backend-vlv-indexes {options}`

1 Description

Lists existing Backend VLV Indexes.

2 Options

The **dsconfig list-backend-vlv-indexes** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--property {property}`

The name of a property to be displayed.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {property}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {unit}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {unit}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

3 Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

The VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig list-backends

dsconfig list-backends — Lists existing Backends

dsconfig list-backends

`dsconfig list-backends {options}`

1 Description

Lists existing Backends.

2 Options

The **dsconfig list-backends** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Backend properties depend on the Backend type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {property}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {property}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {property}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {property}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {property}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {property}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {property}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {property}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {property}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {property}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {property}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {unit}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {unit}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {unit}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {unit}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {unit}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {unit}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {unit}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {unit}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {unit}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {unit}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {unit}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Backend properties depend on the Backend type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {unit}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {unit}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {unit}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {unit}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {unit}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {unit}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {unit}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {unit}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {unit}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {unit}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {unit}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

3 Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or

padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

5 JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an

algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be

used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes

that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk

is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to

the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of

the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

10 PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE

(which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-certificate-mappers

dsconfig list-certificate-mappers — Lists existing Certificate Mappers

dsconfig list-certificate-mappers

`dsconfig list-certificate-mappers {options}`

1 Description

Lists existing Certificate Mappers.

2 Options

The **dsconfig list-certificate-mappers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {property}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {property}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {property}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {property}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {unit}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {unit}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {unit}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {unit}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

3 Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-connection-handlers

dsconfig list-connection-handlers — Lists existing Connection Handlers

dsconfig list-connection-handlers

```
dsconfig list-connection-handlers {options}
```

1 Description

Lists existing Connection Handlers.

2 Options

The **dsconfig list-connection-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Connection Handler properties depend on the Connection Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {property}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {property}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {property}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {property}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {property}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {unit}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {unit}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {unit}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {unit}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {unit}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Connection Handler properties depend on the Connection Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {unit}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {unit}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {unit}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {unit}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {unit}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

3 HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a

very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple

addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept

new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

5 LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure

channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message

may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig list-debug-targets

dsconfig list-debug-targets — Lists existing Debug Targets

dsconfig list-debug-targets

```
dsconfig list-debug-targets {options}
```

1 Description

Lists existing Debug Targets.

2 Options

The **dsconfig list-debug-targets** command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--property {property}`

The name of a property to be displayed.

Debug Target properties depend on the Debug Target type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {property}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {unit}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Debug Target properties depend on the Debug Target type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {unit}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

3 Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-entry-caches

dsconfig list-entry-caches — Lists existing Entry Caches

dsconfig list-entry-caches

```
dsconfig list-entry-caches {options}
```

1 Description

Lists existing Entry Caches.

2 Options

The **dsconfig list-entry-caches** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Entry Cache properties depend on the Entry Cache type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {property}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {property}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {unit}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Entry Cache properties depend on the Entry Cache type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {unit}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {unit}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

3 FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-extended-operation-handlers

dsconfig list-extended-operation-handlers — Lists existing Extended Operation Handlers

dsconfig list-extended-operation-handlers

```
dsconfig list-extended-operation-handlers {options}
```

1 Description

Lists existing Extended Operation Handlers.

2 Options

The **dsconfig list-extended-operation-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {property}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {property}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {property}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {property}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {property}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {property}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {property}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {unit}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {unit}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {unit}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {unit}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {unit}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {unit}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {unit}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

3 Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-group-implementations

dsconfig list-group-implementations — Lists existing Group Implementations

dsconfig list-group-implementations

```
dsconfig list-group-implementations {options}
```

1 Description

Lists existing Group Implementations.

2 Options

The **dsconfig list-group-implementations** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Group Implementation properties depend on the Group Implementation type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {property}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {property}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {property}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {unit}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Group Implementation properties depend on the Group Implementation type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {unit}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {unit}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {unit}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

3 Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-http-authorization-mechanisms

dsconfig list-http-authorization-mechanisms — Lists existing HTTP Authorization Mechanisms

dsconfig list-http-authorization-mechanisms

```
dsconfig list-http-authorization-mechanisms {options}
```

1 Description

Lists existing HTTP Authorization Mechanisms.

2 Options

The **dsconfig list-http-authorization-mechanisms** command takes the following options:

`--property {property}`

The name of a property to be displayed.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {property}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {property}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {property}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {property}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {property}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {property}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {unit}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {unit}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {unit}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {unit}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {unit}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {unit}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

3 HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

8 HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationM

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig list-http-endpoints

dsconfig list-http-endpoints — Lists existing HTTP Endpoints

dsconfig list-http-endpoints

```
dsconfig list-http-endpoints {options}
```

1 Description

Lists existing HTTP Endpoints.

2 Options

The **dsconfig list-http-endpoints** command takes the following options:

`--property {property}`

The name of a property to be displayed.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {property}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {property}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {unit}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {unit}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {unit}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

3 Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es):
org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-identity-mappers

dsconfig list-identity-mappers — Lists existing Identity Mappers

dsconfig list-identity-mappers

`dsconfig list-identity-mappers {options}`

1 Description

Lists existing Identity Mappers.

2 Options

The **dsconfig list-identity-mappers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {property}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {property}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Identity Mapper properties depend on the Identity Mapper type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {unit}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {unit}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

3 Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-key-manager-providers

dsconfig list-key-manager-providers — Lists existing Key Manager Providers

dsconfig list-key-manager-providers

```
dsconfig list-key-manager-providers {options}
```

1 Description

Lists existing Key Manager Providers.

2 Options

The **dsconfig list-key-manager-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {property}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {property}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {property}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {unit}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {unit}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {unit}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

3 File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

5 PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig list-log-publishers

dsconfig list-log-publishers — Lists existing Log Publishers

dsconfig list-log-publishers

```
dsconfig list-log-publishers {options}
```

1 Description

Lists existing Log Publishers.

2 Options

The **dsconfig list-log-publishers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Log Publisher properties depend on the Log Publisher type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {property}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {property}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {property}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {property}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {property}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {property}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {property}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {property}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {property}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {property}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {property}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {unit}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Publisher properties depend on the Log Publisher type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {unit}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {unit}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {unit}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {unit}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {unit}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {unit}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {unit}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {unit}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {unit}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {unit}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {unit}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

3 Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error

warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control,

admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

11 File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true OpenDJ

supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

12 Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-log-retention-policies

dsconfig list-log-retention-policies — Lists existing Log Retention Policies

dsconfig list-log-retention-policies

`dsconfig list-log-retention-policies` {options}

1 Description

Lists existing Log Retention Policies.

2 Options

The **dsconfig list-log-retention-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {property}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {property}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {property}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {unit}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {unit}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {unit}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

3 File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-log-rotation-policies

dsconfig list-log-rotation-policies — Lists existing Log Rotation Policies

dsconfig list-log-rotation-policies

```
dsconfig list-log-rotation-policies {options}
```

1 Description

Lists existing Log Rotation Policies.

2 Options

The **dsconfig list-log-rotation-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {property}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {property}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {property}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {unit}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {unit}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {unit}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

3 Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-monitor-providers

dsconfig list-monitor-providers — Lists existing Monitor Providers

dsconfig list-monitor-providers

```
dsconfig list-monitor-providers {options}
```

1 Description

Lists existing Monitor Providers.

2 Options

The **dsconfig list-monitor-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {property}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {property}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {property}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {property}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {property}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {property}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {unit}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {unit}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Monitor Provider properties depend on the Monitor Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {unit}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {unit}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {unit}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {unit}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {unit}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {unit}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

3 Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-password-generators

dsconfig list-password-generators — Lists existing Password Generators

dsconfig list-password-generators

```
dsconfig list-password-generators {options}
```

1 Description

Lists existing Password Generators.

2 Options

The **dsconfig list-password-generators** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Password Generator properties depend on the Password Generator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {property}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {unit}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Generator properties depend on the Password Generator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {unit}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

3 Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters

are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-password-policies

dsconfig list-password-policies — Lists existing Password Policies

dsconfig list-password-policies

`dsconfig list-password-policies {options}`

1 Description

Lists existing Password Policies.

2 Options

The **dsconfig list-password-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {property}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {property}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {unit}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Authentication Policy properties depend on the Authentication Policy type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {unit}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {unit}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

3 LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the

remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named

attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory

service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds

- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they

become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity

or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-password-storage-schemes

dsconfig list-password-storage-schemes — Lists existing Password Storage Schemes

dsconfig list-password-storage-schemes

```
dsconfig list-password-storage-schemes {options}
```

1 Description

Lists existing Password Storage Schemes.

2 Options

The **dsconfig list-password-storage-schemes** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {property}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {property}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {property}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {property}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {property}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {property}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {property}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {property}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {property}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {property}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {property}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {property}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {property}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {property}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {property}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {property}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {property}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {property}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {unit}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {unit}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {unit}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {unit}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {unit}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {unit}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {unit}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {unit}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {unit}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {unit}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {unit}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {unit}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {unit}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {unit}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {unit}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {unit}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {unit}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

3 AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

15 Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

16 Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

17 Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

18 Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

19 SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

20 Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-password-validators

dsconfig list-password-validators — Lists existing Password Validators

dsconfig list-password-validators

```
dsconfig list-password-validators {options}
```

1 Description

Lists existing Password Validators.

2 Options

The **dsconfig list-password-validators** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Password Validator properties depend on the Password Validator type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {property}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {property}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {property}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {property}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {property}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {property}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {property}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {unit}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {unit}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {unit}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Password Validator properties depend on the Password Validator type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {unit}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {unit}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {unit}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {unit}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {unit}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {unit}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {unit}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

3 Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores

differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-plugins

dsconfig list-plugins — Lists existing Plugins

dsconfig list-plugins

```
dsconfig list-plugins {options}
```

1 Description

Lists existing Plugins.

2 Options

The **dsconfig list-plugins** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Plugin properties depend on the Plugin type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {property}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {property}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {property}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {property}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {property}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {property}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {property}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {property}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {property}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {property}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {property}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {property}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {unit}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {unit}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {unit}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {unit}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {unit}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Plugin properties depend on the Plugin type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {unit}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {unit}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {unit}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {unit}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {unit}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {unit}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {unit}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {unit}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {unit}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {unit}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {unit}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {unit}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

3 Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd

preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that

it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd

postOperationDelete

postOperationModify

postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

7 Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that

it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password

syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Changes to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

11 Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete

postoperationmodifydn

subordinatemodifydn

subordinatedelete

preoperationadd

preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify

postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid

mail

userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preparseadd

preparsemodify

preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

postoperationadd

postoperationmodify

postoperationmodifydn

postsynchronizationadd

postsynchronizationmodify

postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-properties

dsconfig list-properties — Describes managed objects and their properties

dsconfig list-properties

```
dsconfig list-properties {options}
```

1 Description

Describes managed objects and their properties.

2 Options

The **dsconfig list-properties** command takes the following options:

`-c | --category {category}`

The category of components whose properties should be described.

`-t | --type {type}`

The type of components whose properties should be described. The value for TYPE must be one of the component types associated with the CATEGORY specified using the "--category" option.

`--inherited`

Modifies the display output to show the inherited properties of components.

`--property {property}`

The name of a property to be displayed.

dsconfig list-replication-domains

dsconfig list-replication-domains — Lists existing Replication Domains

dsconfig list-replication-domains

```
dsconfig list-replication-domains {options}
```

1 Description

Lists existing Replication Domains.

2 Options

The **dsconfig list-replication-domains** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--property {property}`

The name of a property to be displayed.

Replication Domain properties depend on the Replication Domain type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {property}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {unit}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Domain properties depend on the Replication Domain type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {unit}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

3 Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this

attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts.

When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-replication-server

dsconfig list-replication-server — Lists existing Replication Server

dsconfig list-replication-server

`dsconfig list-replication-server {options}`

1 Description

Lists existing Replication Server.

2 Options

The **dsconfig list-replication-server** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {name}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`--property {property}`

The name of a property to be displayed.

Replication Server properties depend on the Replication Server type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {property}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {unit}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Replication Server properties depend on the Replication Server type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {unit}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

3 Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some

cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new

monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-sasl-mechanism-handlers

dsconfig list-sasl-mechanism-handlers — Lists existing SASL Mechanism Handlers

dsconfig list-sasl-mechanism-handlers

```
dsconfig list-sasl-mechanism-handlers {options}
```

1 Description

Lists existing SASL Mechanism Handlers.

2 Options

The **dsconfig list-sasl-mechanism-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {property}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {property}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {property}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {property}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {property}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {property}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {unit}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {unit}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {unit}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {unit}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {unit}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {unit}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

3 Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then

the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-schema-providers

dsconfig list-schema-providers — Lists existing Schema Providers

dsconfig list-schema-providers

```
dsconfig list-schema-providers {options}
```

1 Description

Lists existing Schema Providers.

2 Options

The **dsconfig list-schema-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Schema Provider properties depend on the Schema Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {property}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {property}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {unit}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {unit}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Schema Provider properties depend on the Schema Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {unit}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {unit}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

3 Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the

revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '*' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig list-service-discovery-mechanisms

dsconfig list-service-discovery-mechanisms — Lists existing Service Discovery Mechanisms

dsconfig list-service-discovery-mechanisms

```
dsconfig list-service-discovery-mechanisms {options}
```

1 Description

Lists existing Service Discovery Mechanisms.

2 Options

The **dsconfig list-service-discovery-mechanisms** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {property}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {property}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {unit}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {unit}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

3 Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

4 Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to

retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig list-synchronization-providers

dsconfig list-synchronization-providers — Lists existing Synchronization Providers

dsconfig list-synchronization-providers

```
dsconfig list-synchronization-providers {options}
```

1 Description

Lists existing Synchronization Providers.

2 Options

The **dsconfig list-synchronization-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {property}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {unit}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

3 Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig list-trust-manager-providers

dsconfig list-trust-manager-providers — Lists existing Trust Manager Providers

dsconfig list-trust-manager-providers

```
dsconfig list-trust-manager-providers {options}
```

1 Description

Lists existing Trust Manager Providers.

2 Options

The **dsconfig list-trust-manager-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {property}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {property}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {property}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {property}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {unit}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {unit}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {unit}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {unit}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

3 Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

6 PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig list-virtual-attributes

dsconfig list-virtual-attributes — Lists existing Virtual Attributes

dsconfig list-virtual-attributes

```
dsconfig list-virtual-attributes {options}
```

1 Description

Lists existing Virtual Attributes.

2 Options

The **dsconfig list-virtual-attributes** command takes the following options:

`--property {property}`

The name of a property to be displayed.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {property} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {property}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {property}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {property}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {property}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {property}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {property}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {property}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {property}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {property}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {property}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {property}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {property}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {property}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {property}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {unit}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, or w (milliseconds, seconds, minutes, hours, days, or weeks).

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {unit} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {unit}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {unit}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {unit}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {unit}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {unit}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {unit}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {unit}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {unit}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {unit}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {unit}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {unit}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {unit}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {unit}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {unit}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

3 Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

10 Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

14 Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

15 Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

16 User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-access-control-handler-prop

dsconfig set-access-control-handler-prop — Modifies Access Control Handler properties

dsconfig set-access-control-handler-prop

```
dsconfig set-access-control-handler-prop {options}
```

1 Description

Modifies Access Control Handler properties.

2 Options

The **dsconfig set-access-control-handler-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Access Control Handler properties depend on the Access Control Handler type, which depends on the null option.

3 Dsee Compat Access Control Handler

Access Control Handlers of type dsee-compat-access-control-handler have the following properties:

enabled

Description

Indicates whether the Access Control Handler is enabled. If set to FALSE, then no access control is enforced, and any client (including unauthenticated or anonymous clients) could be allowed to perform any operation if not subject to other restrictions, such as those enforced by the privilege subsystem.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

global-aci

Description

Defines global access control rules. Global access control rules apply to all entries anywhere in the data managed by the OpenDJ directory server. The global access control rules may be overridden by more specific access control rules placed in the data.

Default Value

No global access control rules are defined, which means that no access is allowed for any data in the server unless specifically granted by access control rules in the data.

Allowed Values

Section 5.1, “About Access Control Instructions”

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dsee Compat Access Control Handler implementation.

Default Value

org.opends.server.authorization.dseecompat.AciHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccessControlHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Access Control Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-access-log-filtering-criteria-prop

dsconfig set-access-log-filtering-criteria-prop — Modifies Access Log Filtering Criteria properties

dsconfig set-access-log-filtering-criteria-prop

```
dsconfig set-access-log-filtering-criteria-prop {options}
```

1 Description

Modifies Access Log Filtering Criteria properties.

2 Options

The **dsconfig set-access-log-filtering-criteria-prop** command takes the following options:

`--publisher-name {name}`

The name of the Access Log Publisher.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Access Log Filtering Criteria types:

access-log-filtering-criteria

Default {name}: Access Log Filtering Criteria

Enabled by default: false

See the section called “Access Log Filtering Criteria” for the properties of this Access Log Filtering Criteria type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Access Log Filtering Criteria properties depend on the Access Log Filtering Criteria type, which depends on the `--criteria-name {name}` option.

3 Access Log Filtering Criteria

Access Log Filtering Criteria of type access-log-filtering-criteria have the following properties:

connection-client-address-equal-to

Description

Filters log records associated with connections which match at least one of the specified client host names or address masks. Valid values

include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-client-address-not-equal-to

Description

Filters log records associated with connections which do not match any of the specified client host names or address masks. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

None

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-port-equal-to

Description

Filters log records associated with connections to any of the specified listener port numbers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-protocol-equal-to

Description

Filters log records associated with connections which match any of the specified protocols. Typical values include "ldap", "ldaps", or "jmx".

Default Value

None

Allowed Values

The protocol name as reported in the access log.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-type

Description

Filters log records based on their type.

Default Value

None

Allowed Values

abandon

Abandon operations

add

Add operations

bind

Bind operations

compare

Compare operations

connect

Client connections

delete

Delete operations

disconnect

Client disconnections

extended

Extended operations

modify

Modify operations

rename

Rename operations

search

Search operations

unbind

Unbind operations

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-equal-to

Description

Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

request-target-dn-not-equal-to

Description

Filters operation log records associated with operations which target entries matching none of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-greater-than

Description

Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-etime-less-than

Description

Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-equal-to

Description

Filters operation response log records associated with operations which include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

response-result-code-not-equal-to

Description

Filters operation response log records associated with operations which do not include any of the specified result codes. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-is-indexed

Description

Filters search operation response log records associated with searches which were either indexed or unindexed. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-greater-than

Description

Filters search operation response log records associated with searches which returned more than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

search-response-nentries-less-than

Description

Filters search operation response log records associated with searches which returned less than the specified number of entries. It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-equal-to

Description

Filters log records associated with users matching at least one of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-dn-not-equal-to

Description

Filters log records associated with users which do not match any of the specified DN patterns. Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more

RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com).

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-member-of

Description

Filters log records associated with users which are members of at least one of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

user-is-not-member-of

Description

Filters log records associated with users which are not members of any of the specified groups.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-account-status-notification-handler-prop

dsconfig set-account-status-notification-handler-prop — Modifies Account Status Notification Handler properties

dsconfig set-account-status-notification-handler-prop

```
dsconfig set-account-status-notification-handler-prop {options}
```

1 Description

Modifies Account Status Notification Handler properties.

2 Options

The **dsconfig set-account-status-notification-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Account Status Notification Handler types:

error-log-account-status-notification-handler

Default {name}: Error Log Account Status Notification Handler

Enabled by default: true

See the section called “Error Log Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

smtp-account-status-notification-handler

Default {name}: SMTP Account Status Notification Handler

Enabled by default: true

See the section called “SMTP Account Status Notification Handler” for the properties of this Account Status Notification Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Account Status Notification Handler properties depend on the Account Status Notification Handler type, which depends on the `--handler-name {name}` option.

3 Error Log Account Status Notification Handler

Account Status Notification Handlers of type error-log-account-status-notification-handler have the following properties:

account-status-notification-type

Description

Indicates which types of event can trigger an account status notification.

Default Value

None

Allowed Values

account-disabled

Generate a notification whenever a user account has been disabled by an administrator.

account-enabled

Generate a notification whenever a user account has been enabled by an administrator.

account-expired

Generate a notification whenever a user authentication has failed because the account has expired.

account-idle-locked

Generate a notification whenever a user account has been locked because it was idle for too long.

account-permanently-locked

Generate a notification whenever a user account has been permanently locked after too many failed attempts.

account-reset-locked

Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.

account-temporarily-locked

Generate a notification whenever a user account has been temporarily locked after too many failed attempts.

account-unlocked

Generate a notification whenever a user account has been unlocked by an administrator.

password-changed

Generate a notification whenever a user changes his/her own password.

password-expired

Generate a notification whenever a user authentication has failed because the password has expired.

password-expiring

Generate a notification whenever a password expiration warning is encountered for a user password for the first time.

password-reset

Generate a notification whenever a user's password is reset by an administrator.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Account Status Notification Handler

Account Status Notification Handlers of type smtp-account-status-notification-handler have the following properties:

email-address-attribute-type

Description

Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified.

Default Value

If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation.

Default Value

org.opends.server.extensions.SMTPAccountStatusNotificationHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AccountStatusNotificationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Account Status Notification Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this account status notification handler. The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-template-file

Description

Specifies the path to the file containing the message template to generate the email notification messages. The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. This may be used to ensure that server administrators also receive a copy of any notification messages that are generated.

Default Value

If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

send-email-as-html

Description

Indicates whether an email notification message should be sent as HTML. If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-message-without-end-user-address

Description

Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

sender-address

Description

Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-administration-connector-prop

dsconfig set-administration-connector-prop — Modifies Administration Connector properties

dsconfig set-administration-connector-prop

```
dsconfig set-administration-connector-prop {options}
```

1 Description

Modifies Administration Connector properties.

2 Options

The **dsconfig set-administration-connector-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Administration Connector properties depend on the Administration Connector type, which depends on the null option.

3 Administration Connector

Administration Connectors of type administration-connector have the following properties:

key-manager-provider

Description

Specifies the name of the key manager that is used with the Administration Connector .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this Administration Connector should listen for connections from LDAP clients. Multiple

addresses may be provided as separate values for this attribute. If no values are provided, then the Administration Connector listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the Administration Connector will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Administration Connector must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Administration Connector should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that is used with the Administration Connector .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

dsconfig set-alert-handler-prop

dsconfig set-alert-handler-prop — Modifies Alert Handler properties

dsconfig set-alert-handler-prop

```
dsconfig set-alert-handler-prop {options}
```

1 Description

Modifies Alert Handler properties.

2 Options

The **dsconfig set-alert-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

Alert Handler properties depend on the Alert Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Alert Handler types:

jmx-alert-handler

Default {name}: JMX Alert Handler

Enabled by default: true

See the section called “JMX Alert Handler” for the properties of this Alert Handler type.

smtp-alert-handler

Default {name}: SMTP Alert Handler

Enabled by default: true

See the section called “SMTP Alert Handler” for the properties of this Alert Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Alert Handler properties depend on the Alert Handler type, which depends on the `--handler-name {name}` option.

3 JMX Alert Handler

Alert Handlers of type jmx-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation.

Default Value

org.opends.server.extensions.JMXAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 SMTP Alert Handler

Alert Handlers of type smtp-alert-handler have the following properties:

disabled-alert-type

Description

Specifies the names of the alert types that are disabled for this alert handler. If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed.

Default Value

If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Alert Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled-alert-type

Description

Specifies the names of the alert types that are enabled for this alert handler. If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed.

Default Value

All alerts with types not included in the set of disabled alert types are allowed.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation.

Default Value

org.opends.server.extensions.SMTPAlertHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AlertHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Alert Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

message-body

Description

Specifies the body that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

message-subject

Description

Specifies the subject that should be used for email messages generated by this alert handler. The token "%%%%alert-type%%%%" is dynamically replaced with the alert type string. The token "%%%%alert-id%%%%" is dynamically replaced with the alert ID value. The token "%%%%alert-message%%%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

recipient-address

Description

Specifies an email address to which the messages should be sent. Multiple values may be provided if there should be more than one recipient.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

sender-address

Description

Specifies the email address to use as the sender for messages generated by this alert handler.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-backend-index-prop

dsconfig set-backend-index-prop — Modifies Backend Index properties

dsconfig set-backend-index-prop

`dsconfig set-backend-index-prop {options}`

1 Description

Modifies Backend Index properties.

2 Options

The **dsconfig set-backend-index-prop** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--index-name {name}`

The name of the Backend Index.

Backend Index properties depend on the Backend Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend Index types:

backend-index

Default {name}: Backend Index

Enabled by default: false

See the section called “Backend Index” for the properties of this Backend Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Backend Index properties depend on the Backend Index type, which depends on the `--index-name {name}` option.

3 Backend Index

Backend Indexes of type backend-index have the following properties:

attribute

Description

Specifies the name of the attribute for which the index is to be maintained.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

confidentiality-enabled

Description

Specifies whether contents of the index should be confidential. Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled.

Advanced Property

No

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit.

Advanced Property

No

Read-only

No

index-extensible-matching-rule

Description

The extensible matching rule in an extensible index. An extensible matching rule must be specified using either LOCALE or OID of the matching rule.

Default Value

No extensible matching rules will be indexed.

Allowed Values

A Locale or an OID.

Multi-valued

Yes

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

No

Read-only

No

index-type

Description

Specifies the type(s) of indexing that should be performed for the associated attribute. For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule.

Default Value

None

Allowed Values

approximate

This index type is used to improve the efficiency of searches using approximate matching search filters.

equality

This index type is used to improve the efficiency of searches using equality search filters.

extensible

This index type is used to improve the efficiency of searches using extensible matching search filters.

ordering

This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.

presence

This index type is used to improve the efficiency of searches using the presence search filters.

substring

This index type is used to improve the efficiency of searches using substring search filters.

Multi-valued

Yes

Required

Yes

Admin Action Required

If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate.

Advanced Property

No

Read-only

No

substring-length

Description

The length of substrings in a substring index.

Default Value

6

Allowed Values

An integer value. Lower value is 3.

Multi-valued

No

Required

No

Admin Action Required

The index must be rebuilt before it will reflect the new value.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-backend-prop

dsconfig set-backend-prop — Modifies Backend properties

dsconfig set-backend-prop

```
dsconfig set-backend-prop {options}
```

1 Description

Modifies Backend properties.

2 Options

The **dsconfig set-backend-prop** command takes the following options:

`--backend-name {name}`

The name of the Backend.

Backend properties depend on the Backend type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend types:

backup-backend

Default {name}: Backup Backend

Enabled by default: true

See the section called “Backup Backend” for the properties of this Backend type.

cas-backend

Default {name}: CAS Backend

Enabled by default: true

See the section called “CAS Backend” for the properties of this Backend type.

je-backend

Default {name}: JE Backend

Enabled by default: true

See the section called “JE Backend” for the properties of this Backend type.

ldif-backend

Default {name}: LDIF Backend

Enabled by default: true

See the section called “LDIF Backend” for the properties of this Backend type.

memory-backend

Default {name}: Memory Backend

Enabled by default: true

See the section called “Memory Backend” for the properties of this Backend type.

monitor-backend

Default {name}: Monitor Backend

Enabled by default: true

See the section called “Monitor Backend” for the properties of this Backend type.

null-backend

Default {name}: Null Backend

Enabled by default: true

See the section called “Null Backend” for the properties of this Backend type.

pdb-backend

Default {name}: PDB Backend

Enabled by default: true

See the section called “PDB Backend” for the properties of this Backend type.

schema-backend

Default {name}: Schema Backend

Enabled by default: true

See the section called “Schema Backend” for the properties of this Backend type.

task-backend

Default {name}: Task Backend

Enabled by default: true

See the section called “Task Backend” for the properties of this Backend type.

trust-store-backend

Default {name}: Trust Store Backend

Enabled by default: true

See the section called “Trust Store Backend” for the properties of this Backend type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Backend properties depend on the Backend type, which depends on the `--backend-name {name}` option.

3 Backup Backend

Backends of type backup-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

backup-directory

Description

Specifies the path to a backup directory containing one or more backups for a particular backend. This is a multivalued property. Each value may specify a different backup directory if desired (one for each backend for which backups are taken). Values may be either absolute paths or paths that are relative to the base of the OpenDJ directory server installation.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.BackupBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 CAS Backend

Backends of type cas-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-directory

Description

Specifies the keyspace name The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

ldap_opendj

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the

backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.cassandra.Backend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

5 JE Backend

Backends of type je-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise,

the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-bytes-interval

Description

Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero.

Default Value

500mb

Allowed Values

Upper value is 9223372036854775807.

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. Note that this is only used if the value of the checkpointer bytes interval is zero.

Default Value

30s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 4294 seconds.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-cleaner-min-utilization

Description

Specifies the occupancy percentage for "live" data in this backend's database. When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database.

Default Value

50

Allowed Values

An integer value. Lower value is 0. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this

backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-core-threads

Description

Specifies the core number of threads in the eviction thread pool. Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

1

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-keep-alive

Description

The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

600s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.Upper limit is 86400 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-lru-only

Description

Indicates whether the database should evict existing data from the cache based on an LRU policy (where the least recently used information will be evicted first). If set to "false", then the eviction keeps internal nodes of the underlying Btree in the cache over leaf nodes, even if the leaf nodes have been accessed more recently. This may be a better configuration for databases in which only a very small portion of the data is cached.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-max-threads

Description

Specifies the maximum number of threads in the eviction thread pool. Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-evictor-nodes-per-scan

Description

Specifies the number of Btree nodes that should be evicted from the cache in a single pass if it is determined that it is necessary to free existing data in order to make room for new information. Changes to this property do not take effect until the backend is restarted. It is recommended that you also change this property when you set db-evictor-lru-only to false. This setting controls the number of Btree nodes that are considered, or sampled, each time a node is evicted. A setting of 10 often produces good results, but this may vary from application to application. The larger the nodes per scan, the more accurate the algorithm. However, don't set it too high. When considering larger numbers of nodes for each eviction, the evictor may delay the completion of a given database operation, which impacts the response time of the application thread. In JE 4.1 and later, setting this value too high in an application that is largely CPU bound can reduce the effectiveness of cache eviction. It's best to start with the default value, and increase it gradually to see if it is beneficial for your application.

Default Value

10

Allowed Values

An integer value. Lower value is 1. Upper value is 1000.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-file-max

Description

Specifies the maximum size for a database log file.

Default Value

100mb

Allowed Values

Lower value is 1000000.Upper value is 4294967296.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-log-filecache-size

Description

Specifies the size of the file handle cache. The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately.

Default Value

100

Allowed Values

An integer value. Lower value is 3. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-file-handler-on

Description

Indicates whether the database should maintain a je.info file in the same directory as the database log directory. This file contains information about the internal processing performed by the underlying database.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-logging-level

Description

Specifies the log level that should be used by the database when it is writing information into the je.info file. The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL.

Default Value

CONFIG

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-cleaner-threads

Description

Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-num-lock-tables

Description

Specifies the number of lock tables that are used by the underlying database. This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 32767.

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-run-cleaner

Description

Indicates whether the cleaner threads should be enabled to compact the database. The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-write-no-sync

Description

Indicates whether the database should synchronously flush data as it is written to disk. If this value is set to "false", then all data written to disk is synchronously flushed to persistent storage and thereby providing full durability. If it is set to "true", then data may be cached for a period of time by the underlying operating system before actually being written to disk. This may improve performance, but could cause the most recent changes to be lost in the event of an underlying OS or hardware failure (but not in the case that the OpenDJ directory server or the JVM exits abnormally).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.jeb.JEBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

je-property

Description

Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further

information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 LDIF Backend

Backends of type ldif-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

is-private-backend

Description

Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.LDIFBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-file

Description

Specifies the path to the LDIF file containing the data for this backend.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Memory Backend

Backends of type memory-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a

base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MemoryBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Monitor Backend

Backends of type monitor-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a

base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.MonitorBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

disabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Null Backend

Backends of type null-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a

base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.NullBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

10 PDB Backend

Backends of type pdb-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two

backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compact-encoding

Description

Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. Note that this property applies only to the entries themselves and does not impact the index data.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the backend should make entries in database files readable only by Directory Server. Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-percent

Description

Specifies the percentage of JVM memory to allocate to the database cache. Specifies the percentage of memory available to the JVM that

should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration.

Default Value

50

Allowed Values

An integer value. Lower value is 1. Upper value is 90.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-cache-size

Description

The amount of JVM memory to allocate to the database cache. Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size.

Default Value

0 MB

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

db-checkpointer-wakeup-interval

Description

Specifies the maximum length of time that may pass between checkpoints. This setting controls the elapsed time between attempts to write a checkpoint to the journal. A longer interval allows more updates to accumulate in buffers before they are required to be written to disk, but also potentially causes recovery from an abrupt termination (crash) to take more time.

Default Value

15s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days

- `w`: weeks

  Lower limit is 10 seconds.Upper limit is 3600 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-directory

Description

Specifies the path to the filesystem directory that is used to hold the Persistit database files containing the data for this backend. The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents.

Default Value

db

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

db-directory-permissions

Description

Specifies the permissions that should be applied to the directory containing the server database files. They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files.

Default Value

700

Allowed Values

Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory).

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

db-txn-no-sync

Description

Indicates whether database writes should be primarily written to an internal buffer but not immediately written to disk. Setting the value of this configuration attribute to "true" may improve write performance but could cause the most recent changes to be lost if the OpenDJ directory server or the underlying JVM exits abnormally, or if an OS or hardware failure occurs (a behavior similar to running with transaction durability disabled in the Sun Java System Directory Server).

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-full-threshold

Description

Full disk threshold to limit database updates When the available free space on the disk used by this database instance falls below the

value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold.

Default Value

100 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disk-low-threshold

Description

Low disk threshold to limit database updates Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege.

Default Value

200 megabytes

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

entries-compressed

Description

Indicates whether the backend should attempt to compress entries before storing them in the database. Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

import-offheap-memory-size

Description

Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index).

Default Value

Use only heap memory.

Allowed Values

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-entry-limit

Description

Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis.A value of 0 means there is no limit.

Default Value

4000

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit.

Advanced Property

No

Read-only

No

index-filter-analyzer-enabled

Description

Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

index-filter-analyzer-max-filters

Description

The maximum number of search filter statistics to keep. When the maximum number of search filter is reached, the least used one will be deleted.

Default Value

25

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.pdb.PDBBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

preload-time-limit

Description

Specifies the length of time that the backend is allowed to spend "pre-loading" data when it is initialized. The pre-load process is used to pre-populate the database cache, so that it can be more quickly available when the server is processing requests. A duration of zero means there is no pre-load.

Default Value

0s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Schema Backend

Backends of type schema-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.SchemaBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

schema-entry-dn

Description

Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE

(which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location.

Default Value

cn=schema

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

show-all-attributes

Description

Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Task Backend

Backends of type task-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.task.TaskBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

notification-sender-address

Description

Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution.

Default Value

The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

task-backing-file

Description

Specifies the path to the backing file for storing information about the tasks configured in the server. It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

task-retention-time

Description

Specifies the length of time that task entries should be retained after processing on the associated task has been completed.

Default Value

24 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Trust Store Backend

Backends of type trust-store-backend have the following properties:

backend-id

Description

Specifies a name to identify the associated backend. The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

base-dn

Description

Specifies the base DN(s) for the data that the backend handles. A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the backend is enabled in the server. If a backend is not enabled, then its contents are not accessible when processing operations.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the backend implementation.

Default Value

org.opends.server.backends.TrustStoreBackend

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Backend

Multi-valued

No

Required

Yes

Admin Action Required

The Backend must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file that stores the trust information. It may be an absolute path, or a path that is relative to the OpenDJ instance root.

Default Value

config/ads-truststore

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the Trust Store Backend .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Trust Store Backend is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well.

Default Value

The JVM default value is used.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect the next time that the key manager is accessed.

Advanced Property

No

Read-only

No

writability-mode

Description

Specifies the behavior that the backend should use when processing write operations.

Default Value

enabled

Allowed Values

disabled

Causes all write attempts to fail.

enabled

Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).

internal-only

Causes external write attempts to fail but allows writes by replication and internal operations.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-backend-vlv-index-prop

dsconfig set-backend-vlv-index-prop — Modifies Backend VLV Index properties

dsconfig set-backend-vlv-index-prop

```
dsconfig set-backend-vlv-index-prop {options}
```

1 Description

Modifies Backend VLV Index properties.

2 Options

The **dsconfig set-backend-vlv-index-prop** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--index-name {name}`

The name of the Backend VLV Index.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Backend VLV Index types:

backend-vlv-index

Default {name}: Backend VLV Index

Enabled by default: false

See the section called “Backend VLV Index” for the properties of this Backend VLV Index type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Backend VLV Index properties depend on the Backend VLV Index type, which depends on the `--index-name {name}` option.

3 Backend VLV Index

Backend VLV Indexes of type backend-vlv-index have the following properties:

base-dn

Description

Specifies the base DN used in the search query that is being indexed.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

filter

Description

Specifies the LDAP filter used in the query that is being indexed.

Default Value

None

Allowed Values

A valid LDAP search filter.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

name

Description

Specifies a unique name for this VLV index.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

The VLV index name cannot be altered after the index is created.

Advanced Property

No

Read-only

Yes

scope

Description

Specifies the LDAP scope of the query that is being indexed.

Default Value

None

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

sort-order

Description

Specifies the names of the attributes that are used to sort the entries for the query being indexed. Multiple attributes can be used to determine

the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively.

Default Value

None

Allowed Values

Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -.

Multi-valued

No

Required

Yes

Admin Action Required

The index must be rebuilt after modifying this property.

Advanced Property

No

Read-only

No

dsconfig set-certificate-mapper-prop

dsconfig set-certificate-mapper-prop — Modifies Certificate Mapper properties

dsconfig set-certificate-mapper-prop

```
dsconfig set-certificate-mapper-prop {options}
```

1 Description

Modifies Certificate Mapper properties.

2 Options

The **dsconfig set-certificate-mapper-prop** command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Certificate Mapper types:

fingerprint-certificate-mapper

Default {name}: Fingerprint Certificate Mapper

Enabled by default: true

See the section called “Fingerprint Certificate Mapper” for the properties of this Certificate Mapper type.

subject-attribute-to-user-attribute-certificate-mapper

Default {name}: Subject Attribute To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject Attribute To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-dn-to-user-attribute-certificate-mapper

Default {name}: Subject DN To User Attribute Certificate Mapper

Enabled by default: true

See the section called “Subject DN To User Attribute Certificate Mapper” for the properties of this Certificate Mapper type.

subject-equals-dn-certificate-mapper

Default {name}: Subject Equals DN Certificate Mapper

Enabled by default: true

See the section called “Subject Equals DN Certificate Mapper” for the properties of this Certificate Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Certificate Mapper properties depend on the Certificate Mapper type, which depends on the `--mapper-name {name}` option.

3 Fingerprint Certificate Mapper

Certificate Mappers of type fingerprint-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-algorithm

Description

Specifies the name of the digest algorithm to compute the fingerprint of client certificates.

Default Value

None

Allowed Values

md5

Use the MD5 digest algorithm to compute certificate fingerprints.

sha1

Use the SHA-1 digest algorithm to compute certificate fingerprints.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

fingerprint-attribute

Description

Specifies the attribute in which to look for the fingerprint. Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation.

Default Value

org.opends.server.extensions.FingerprintCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs are used when performing searches to map the client certificates to a user entry.

Default Value

The server performs the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Subject Attribute To User Attribute Certificate Mapper

Certificate Mappers of type subject-attribute-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute-mapping

Description

Specifies a mapping between certificate attributes and user attributes. Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Subject DN To User Attribute Certificate Mapper

Certificate Mappers of type subject-dn-to-user-attribute-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

subject-attribute

Description

Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

user-base-dn

Description

Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry.

Default Value

The server will perform the search in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Subject Equals DN Certificate Mapper

Certificate Mappers of type subject-equals-dn-certificate-mapper have the following properties:

enabled

Description

Indicates whether the Certificate Mapper is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation.

Default Value

org.opends.server.extensions.SubjectEqualsDNCertificateMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.CertificateMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Certificate Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-connection-handler-prop

dsconfig set-connection-handler-prop — Modifies Connection Handler properties

dsconfig set-connection-handler-prop

```
dsconfig set-connection-handler-prop {options}
```

1 Description

Modifies Connection Handler properties.

2 Options

The **dsconfig set-connection-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

Connection Handler properties depend on the Connection Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Connection Handler types:

http-connection-handler

Default {name}: HTTP Connection Handler

Enabled by default: true

See the section called “HTTP Connection Handler” for the properties of this Connection Handler type.

jmx-connection-handler

Default {name}: JMX Connection Handler

Enabled by default: true

See the section called “JMX Connection Handler” for the properties of this Connection Handler type.

ldap-connection-handler

Default {name}: LDAP Connection Handler

Enabled by default: true

See the section called “LDAP Connection Handler” for the properties of this Connection Handler type.

ldif-connection-handler

Default {name}: LDIF Connection Handler

Enabled by default: true

See the section called “LDIF Connection Handler” for the properties of this Connection Handler type.

snmp-connection-handler

Default {name}: SNMP Connection Handler

Enabled by default: true

See the section called “SNMP Connection Handler” for the properties of this Connection Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Connection Handler properties depend on the Connection Handler type, which depends on the `--handler-name {name}` option.

3 HTTP Connection Handler

Connection Handlers of type http-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the HTTP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the HTTP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation.

Default Value

org.opends.server.protocols.http.HTTPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the HTTP Connection Handler should keep statistics. If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this HTTP Connection Handler should listen for connections from HTTP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the HTTP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-concurrent-ops-per-connection

Description

Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL

communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the HTTP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the HTTP Connection Handler should use SSL. If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the HTTP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the HTTP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 JMX Connection Handler

Connection Handlers of type jmx-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation.

Default Value

org.opends.server.protocols.jmx.JmxConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this JMX Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. If no value is provided, then the JMX Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the JMX Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

rmi-port

Description

Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the JMX Connection Handler should use SSL. If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

5 LDAP Connection Handler

Connection Handlers of type ldap-connection-handler have the following properties:

accept-backlog

Description

Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established.

Default Value

128

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-ldap-v2

Description

Indicates whether connections from LDAPv2 clients are allowed. If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-start-tls

Description

Indicates whether clients are allowed to use StartTLS. If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended

operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-tcp-reuse-address

Description

Indicates whether the LDAP Connection Handler should reuse socket descriptors. If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

buffer-size

Description

Specifies the size in bytes of the LDAP response message write buffer. This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing.

Default Value

4096 bytes

Allowed Values

Lower value is 1.Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation.

Default Value

org.opends.server.protocols.ldap.LDAPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

keep-stats

Description

Indicates whether the LDAP Connection Handler should keep statistics. If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this LDAP Connection Handler .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this LDAP Connection Handler should listen for connections from LDAP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the LDAP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

listen-port

Description

Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

max-blocked-write-time-limit

Description

Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated.

Default Value

2 minutes

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-request-size

Description

Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory.

Default Value

5 megabytes

Allowed Values

Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-request-handlers

Description

Specifies the number of request handlers that are used to read requests from clients. The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

send-rejection-notice

Description

Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. The extended response message

may provide an explanation indicating the reason that the connection was rejected.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-client-auth-policy

Description

Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". This is only applicable if clients are allowed to use SSL.

Default Value

optional

Allowed Values

disabled

Clients must not provide their own certificates when performing SSL negotiation.

optional

Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.

required

Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the LDAP Connection Handler .

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Connection Handler should use SSL. If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether the LDAP Connection Handler should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether the LDAP Connection Handler should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 LDIF Connection Handler

Connection Handlers of type ldif-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation.

Default Value

org.opends.server.protocols.LDIFConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ldif-directory

Description

Specifies the path to the directory in which the LDIF files should be placed.

Default Value

config/auto-process-ldif

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

poll-interval

Description

Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 SNMP Connection Handler

Connection Handlers of type snmp-connection-handler have the following properties:

allowed-client

Description

Specifies a set of host names or address masks that determine the clients that are allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask.

Default Value

All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

allowed-manager

Description

Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

allowed-user

Description

Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users.

Default Value

*

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

community

Description

Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

denied-client

Description

Specifies a set of host names or address masks that determine the clients that are not allowed to establish connections to this Connection Handler. Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed.

Default Value

If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed.

Allowed Values

An IP address mask

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately and do not interfere with connections that may have already been established.

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Connection Handler is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation.

Default Value

org.opends.server.snmp.SNMPConnectionHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ConnectionHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

listen-address

Description

Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces.

Default Value

0.0.0.0

Allowed Values

An IP address

Multi-valued

Yes

Required

No

Admin Action Required

Restart the server

Advanced Property

No

Read-only

Yes

listen-port

Description

Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. Only a single port number may be provided.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

opendmk-jarfile

Description

Indicates the OpenDMK runtime jar file location

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

registered-mbean

Description

Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-agent-file

Description

Specifies the USM security configuration to receive authenticated only SNMP requests.

Default Value

config/snmp/security/opendj-snmp.security

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

security-level

Description

Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration.

Default Value

authnopriv

Allowed Values

authnopriv

Authentication activated with no privacy.

authpriv

Authentication with privacy activated.

noauthnopriv

No security mechanisms activated.

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trap-port

Description

Specifies the port to use to send SNMP Traps.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-community

Description

Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3.

Default Value

OpenDJ

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

traps-destination

Description

Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess.

Default Value

If the list is empty, V1 traps are sent to "localhost".

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Connection Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig set-crypto-manager-prop

dsconfig set-crypto-manager-prop — Modifies Crypto Manager properties

dsconfig set-crypto-manager-prop

```
dsconfig set-crypto-manager-prop {options}
```

1 Description

Modifies Crypto Manager properties.

2 Options

The **dsconfig set-crypto-manager-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Crypto Manager properties depend on the Crypto Manager type, which depends on the null option.

3 Crypto Manager

Crypto Managers of type crypto-manager have the following properties:

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server using the syntax algorithm/mode/padding. The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these

default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

digest-algorithm

Description

Specifies the preferred message digest algorithm for the directory server.

Default Value

SHA-256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately and only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-wrapping-transformation

Description

The preferred key wrapping transformation for the directory server. This value must be the same for all server instances in a replication topology.

Default Value

RSA/ECB/OAEPWITHSHA-1ANDMGF1PADDING

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect immediately but will only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

mac-algorithm

Description

Specifies the preferred MAC algorithm for the directory server.

Default Value

HmacSHA256

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mac-key-length

Description

Specifies the key length in bits for the preferred MAC algorithm.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Crypto Manager should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Crypto Manager is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Crypto Manager must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-encryption

Description

Specifies whether SSL/TLS is used to provide encrypted communication between two OpenDJ server components.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change.

Advanced Property

No

Read-only

No

dsconfig set-debug-target-prop

dsconfig set-debug-target-prop — Modifies Debug Target properties

dsconfig set-debug-target-prop

```
dsconfig set-debug-target-prop {options}
```

1 Description

Modifies Debug Target properties.

2 Options

The **dsconfig set-debug-target-prop** command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--target-name {name}`

The name of the Debug Target.

Debug Target properties depend on the Debug Target type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Debug Target types:

debug-target

Default {name}: Debug Target

Enabled by default: true

See the section called “Debug Target” for the properties of this Debug Target type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Debug Target properties depend on the Debug Target type, which depends on the `--target-name {name}` option.

3 Debug Target

Debug Targets of type debug-target have the following properties:

debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

debug-scope

Description

Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Default Value

None

Allowed Values

The fully-qualified OpenDJ Java package, class, or method name.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the Debug Target is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

include-throwable-cause

Description

Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-entry-arguments

Description

Specifies the property to indicate whether to include method arguments in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

omit-method-return-value

Description

Specifies the property to indicate whether to include the return value in debug messages.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

throwable-stack-frames

Description

Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-entry-cache-prop

dsconfig set-entry-cache-prop — Modifies Entry Cache properties

dsconfig set-entry-cache-prop

```
dsconfig set-entry-cache-prop {options}
```

1 Description

Modifies Entry Cache properties.

2 Options

The **dsconfig set-entry-cache-prop** command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

Entry Cache properties depend on the Entry Cache type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Entry Cache types:

fifo-entry-cache

Default {name}: FIFO Entry Cache

Enabled by default: true

See the section called “FIFO Entry Cache” for the properties of this Entry Cache type.

soft-reference-entry-cache

Default {name}: Soft Reference Entry Cache

Enabled by default: true

See the section called “Soft Reference Entry Cache” for the properties of this Entry Cache type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Entry Cache properties depend on the Entry Cache type, which depends on the `--cache-name {name}` option.

3 FIFO Entry Cache

Entry Caches of type fifo-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation.

Default Value

org.opends.server.extensions.FIFOEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time to wait while attempting to acquire a read or write lock.

Default Value

2000.0ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-entries

Description

Specifies the maximum number of entries that we will allow in the cache.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-memory-percent

Description

Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely.

Default Value

90

Allowed Values

An integer value. Lower value is 1. Upper value is 100.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Soft Reference Entry Cache

Entry Caches of type soft-reference-entry-cache have the following properties:

cache-level

Description

Specifies the cache level in the cache order if more than one instance of the cache is configured.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Entry Cache is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

exclude-filter

Description

The set of filters that define the entries that should be excluded from the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

include-filter

Description

The set of filters that define the entries that should be included in the cache.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation.

Default Value

org.opends.server.extensions.SoftReferenceEntryCache

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.EntryCache

Multi-valued

No

Required

Yes

Admin Action Required

The Entry Cache must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lock-timeout

Description

Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock.

Default Value

3000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

A value of "-1" or "unlimited" for no limit. Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-extended-operation-handler-prop

dsconfig set-extended-operation-handler-prop — Modifies Extended Operation Handler properties

dsconfig set-extended-operation-handler-prop

```
dsconfig set-extended-operation-handler-prop {options}
```

1 Description

Modifies Extended Operation Handler properties.

2 Options

The **dsconfig set-extended-operation-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Extended Operation Handler types:

cancel-extended-operation-handler

Default {name}: Cancel Extended Operation Handler

Enabled by default: true

See the section called “Cancel Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-connection-id-extended-operation-handler

Default {name}: Get Connection Id Extended Operation Handler

Enabled by default: true

See the section called “Get Connection Id Extended Operation Handler” for the properties of this Extended Operation Handler type.

get-symmetric-key-extended-operation-handler

Default {name}: Get Symmetric Key Extended Operation Handler

Enabled by default: true

See the section called “Get Symmetric Key Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-modify-extended-operation-handler

Default {name}: Password Modify Extended Operation Handler

Enabled by default: true

See the section called “Password Modify Extended Operation Handler” for the properties of this Extended Operation Handler type.

password-policy-state-extended-operation-handler

Default {name}: Password Policy State Extended Operation Handler

Enabled by default: true

See the section called “Password Policy State Extended Operation Handler” for the properties of this Extended Operation Handler type.

start-tls-extended-operation-handler

Default {name}: Start TLS Extended Operation Handler

Enabled by default: true

See the section called “Start TLS Extended Operation Handler” for the properties of this Extended Operation Handler type.

who-am-i-extended-operation-handler

Default {name}: Who Am I Extended Operation Handler

Enabled by default: true

See the section called “Who Am I Extended Operation Handler” for the properties of this Extended Operation Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Extended Operation Handler properties depend on the Extended Operation Handler type, which depends on the `--handler-name {name}` option.

3 Cancel Extended Operation Handler

Extended Operation Handlers of type cancel-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.CancelExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Get Connection Id Extended Operation Handler

Extended Operation Handlers of type get-connection-id-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Connection Id Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.GetConnectionIDExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Get Symmetric Key Extended Operation Handler

Extended Operation Handlers of type get-symmetric-key-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation.

Default Value

org.opends.server.crypto.GetSymmetricKeyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Password Modify Extended Operation Handler

Extended Operation Handlers of type password-modify-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that should be used in conjunction with the password modify extended operation. This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Password Modify Extended Operation Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordModifyExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Password Policy State Extended Operation Handler

Extended Operation Handlers of type password-policy-state-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.PasswordPolicyStateExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Start TLS Extended Operation Handler

Extended Operation Handlers of type start-tls-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Start TLS Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.StartTLSExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Who Am I Extended Operation Handler

Extended Operation Handlers of type who-am-i-extended-operation-handler have the following properties:

enabled

Description

Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server).

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation.

Default Value

org.opends.server.extensions.WhoAmIExtendedOperation

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.ExtendedOperationHandler

Multi-valued

No

Required

Yes

Admin Action Required

The Extended Operation Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-external-changelog-domain-prop

dsconfig set-external-changelog-domain-prop — Modifies External Changelog Domain properties

dsconfig set-external-changelog-domain-prop

```
dsconfig set-external-changelog-domain-prop {options}
```

1 Description

Modifies External Changelog Domain properties.

2 Options

The **dsconfig set-external-changelog-domain-prop** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {name}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`--domain-name {name}`

The name of the Replication Domain.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following External Changelog Domain types:

external-changelog-domain

Default {name}: External Changelog Domain

Enabled by default: true

See the section called “External Changelog Domain” for the properties of this External Changelog Domain type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

External Changelog Domain properties depend on the External Changelog Domain type, which depends on the `--domain-name {name}` option.

3 External Changelog Domain

External Changelog Domains of type external-changelog-domain have the following properties:

ecl-include

Description

Specifies a list of attributes which should be published with every change log entry, regardless of whether the attribute itself has changed. The list

of attributes may include wild cards such as "*" and "+" as well as object class references prefixed with an ampersand, for example "@person". The included attributes will be published using the "includedAttributes" operational attribute as a single LDIF value rather like the "changes" attribute. For modify and modifyDN operations the included attributes will be taken from the entry before any changes were applied.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ecl-include-for-deletes

Description

Specifies a list of attributes which should be published with every delete operation change log entry, in addition to those specified by the "ecl-include" property. This property provides a means for applications to archive entries after they have been deleted. See the description of the "ecl-include" property for further information about how the included attributes are published.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the External Changelog Domain is enabled. To enable computing the change numbers, set the Replication Server's "ds-cfg-compute-change-number" property to true.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-global-configuration-prop

dsconfig set-global-configuration-prop — Modifies Global Configuration properties

dsconfig set-global-configuration-prop

```
dsconfig set-global-configuration-prop {options}
```

1 Description

Modifies Global Configuration properties.

2 Options

The **dsconfig set-global-configuration-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Global Configuration properties depend on the Global Configuration type, which depends on the null option.

3 Global Configuration

Global Configurations of type global have the following properties:

add-missing-rdn-attributes

Description

Indicates whether the directory server should automatically add any attribute values contained in the entry's RDN into that entry when processing an add request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-attribute-name-exceptions

Description

Indicates whether the directory server should allow underscores in attribute names and allow attribute names to begin with numeric digits (both of which are violations of the LDAP standards).

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allowed-task

Description

Specifies the fully-qualified name of a Java class that may be invoked in the server. Any attempt to invoke a task not included in the list of allowed tasks is rejected.

Default Value

If no values are defined, then the server does not allow any tasks to be invoked.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

bind-with-dn-requires-password

Description

Indicates whether the directory server should reject any simple bind request that contains a DN but no password. Although such bind requests are technically allowed by the LDAPv3 specification (and should be treated as anonymous simple authentication), they may introduce security problems in applications that do not verify that the client actually provided a password.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-schema

Description

Indicates whether schema enforcement is active. When schema enforcement is activated, the directory server ensures that all operations result in entries are valid according to the defined server schema. It is strongly recommended that this option be left enabled to prevent the inadvertent addition of invalid data into the server.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-password-policy

Description

Specifies the name of the password policy that is in effect for users whose entries do not specify an alternate password policy (either via a real or

virtual attribute). In addition, the default password policy will be used for providing default parameters for sub-entry based password policies when not provided or supported by the sub-entry itself. This property must reference a password policy and no other type of authentication policy.

Default Value

None

Allowed Values

The DN of any Password Policy.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-privilege

Description

Specifies the name of a privilege that should not be evaluated by the server. If a privilege is disabled, then it is assumed that all clients (including unauthenticated clients) have that privilege.

Default Value

If no values are defined, then the server enforces all privileges.

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

The privilege that provides the ability to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

etime-resolution

Description

Specifies the resolution to use for operation elapsed processing time (etime) measurements.

Default Value

milliseconds

Allowed Values

milliseconds

Use millisecond resolution.

nanoseconds

Use nanosecond resolution.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-time-limit

Description

Specifies the maximum length of time that a client connection may remain established since its last completed operation. A value of "0 seconds" indicates that no idle time limit is enforced.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

invalid-attribute-syntax-behavior

Description

Specifies how the directory server should handle operations whenever an attribute value violates the associated attribute syntax.

Default Value

reject

Allowed Values

accept

The directory server silently accepts attribute values that are invalid according to their associated syntax. Matching operations targeting those values may not behave as expected.

reject

The directory server rejects attribute values that are invalid according to their associated syntax.

warn

The directory server accepts attribute values that are invalid according to their associated syntax, but also logs a warning message to the error log. Matching operations targeting those values may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

lookthrough-limit

Description

Specifies the maximum number of entries that the directory server should "look through" in the course of processing a search request. This includes any entry that the server must examine in the course of processing the request, regardless of whether it actually matches the search criteria. A value of 0 indicates that no lookthrough limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-lookthrough-limit operational attribute.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-allowed-client-connections

Description

Specifies the maximum number of client connections that may be established at any given time A value of 0 indicates that unlimited client connection is allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-internal-buffer-size

Description

The threshold capacity beyond which internal cached buffers used for encoding and decoding entries and protocol messages will be trimmed after use. Individual buffers may grow very large when encoding and decoding large entries and protocol messages and should be reduced in size when they are no longer needed. This setting specifies the threshold at which a buffer is determined to have grown too big and should be trimmed down after use.

Default Value

32 KB

Allowed Values

Lower value is 512.Upper value is 1000000000.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-psearches

Description

Defines the maximum number of concurrent persistent searches that can be performed on directory server The persistent search mechanism provides an active channel through which entries that change, and information about the changes that occur, can be communicated. Because each persistent search operation consumes resources, limiting the number of simultaneous persistent searches keeps the performance impact minimal. A value of -1 indicates that there is no limit on the persistent searches.

Default Value

-1

Allowed Values

An integer value. Lower value is 0. A value of "-1" or "unlimited" for no limit.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

notify-abandoned-operations

Description

Indicates whether the directory server should send a response to any operation that is interrupted via an abandon request. The LDAP specification states that abandoned operations should not receive any response, but this may cause problems with client applications that always expect to receive a response to each request.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

proxied-authorization-identity-mapper

Description

Specifies the name of the identity mapper to map authorization ID values (using the "u:" form) provided in the proxied authorization control to the corresponding user entry.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

reject-unauthenticated-requests

Description

Indicates whether the directory server should reject any request (other than bind or StartTLS requests) received from a client that has not yet been authenticated, whose last authentication attempt was unsuccessful, or whose last authentication attempt used anonymous authentication.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

return-bind-error-messages

Description

Indicates whether responses for failed bind operations should include a message string providing the reason for the authentication failure. Note that these messages may include information that could potentially be used by an attacker. If this option is disabled, then these messages appears only in the server's access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

save-config-on-successful-startup

Description

Indicates whether the directory server should save a copy of its configuration whenever the startup process completes successfully. This ensures that the server provides a "last known good" configuration, which can be used as a reference (or copied into the active config) if the server fails to start with the current "active" configuration.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-error-result-code

Description

Specifies the numeric value of the result code when request processing fails due to an internal server error.

Default Value

80

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

single-structural-objectclass-behavior

Description

Specifies how the directory server should handle operations an entry does not contain a structural object class or contains multiple structural classes.

Default Value

reject

Allowed Values

accept

The directory server silently accepts entries that do not contain exactly one structural object class. Certain schema features that depend on the entry's structural class may not behave as expected.

reject

The directory server rejects entries that do not contain exactly one structural object class.

warn

The directory server accepts entries that do not contain exactly one structural object class, but also logs a warning message to the error log. Certain schema features that depend on the entry's structural class may not behave as expected.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

size-limit

Description

Specifies the maximum number of entries that can be returned to the client during a single search operation. A value of 0 indicates that no size

limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-size-limit operational attribute.

Default Value

1000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

smtp-server

Description

Specifies the address (and optional port number) for a mail server that can be used to send email messages via SMTP. It may be an IP address or resolvable hostname, optionally followed by a colon and a port number.

Default Value

If no values are defined, then the server cannot send email via SMTP.

Allowed Values

A hostname, optionally followed by a ":" followed by a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

subordinate-base-dn

Description

Specifies the set of base DNs used for singleLevel, wholeSubtree, and subordinateSubtree searches based at the root DSE.

Default Value

The set of all user-defined suffixes is used.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-limit

Description

Specifies the maximum length of time that should be spent processing a single search operation. A value of 0 seconds indicates that no time limit is enforced. Note that this is the default server-wide time limit, but it may be overridden on a per-user basis using the ds-rlim-time-limit operational attribute.

Default Value

60 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-transaction-ids

Description

Indicates whether the directory server should trust the transaction ids that may be received from requests, either through a LDAP control or through a HTTP header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

writability-mode

Description

Specifies the kinds of write operations the directory server can process.

Default Value

enabled

Allowed Values

disabled

The directory server rejects all write operations that are requested of it, regardless of their origin.

enabled

The directory server attempts to process all write operations that are requested of it, regardless of their origin.

internal-only

The directory server attempts to process write operations requested as internal operations or through synchronization, but rejects any such operations requested from external clients.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-group-implementation-prop

dsconfig set-group-implementation-prop — Modifies Group Implementation properties

dsconfig set-group-implementation-prop

```
dsconfig set-group-implementation-prop {options}
```

1 Description

Modifies Group Implementation properties.

2 Options

The **dsconfig set-group-implementation-prop** command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

Group Implementation properties depend on the Group Implementation type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Group Implementation types:

dynamic-group-implementation

Default {name}: Dynamic Group Implementation

Enabled by default: true

See the section called “Dynamic Group Implementation” for the properties of this Group Implementation type.

static-group-implementation

Default {name}: Static Group Implementation

Enabled by default: true

See the section called “Static Group Implementation” for the properties of this Group Implementation type.

virtual-static-group-implementation

Default {name}: Virtual Static Group Implementation

Enabled by default: true

See the section called “Virtual Static Group Implementation” for the properties of this Group Implementation type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Group Implementation properties depend on the Group Implementation type, which depends on the `--implementation-name {name}` option.

3 Dynamic Group Implementation

Group Implementations of type dynamic-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation.

Default Value

org.opends.server.extensions.DynamicGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Static Group Implementation

Group Implementations of type static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation.

Default Value

org.opends.server.extensions.StaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Virtual Static Group Implementation

Group Implementations of type virtual-static-group-implementation have the following properties:

enabled

Description

Indicates whether the Group Implementation is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation.

Default Value

org.opends.server.extensions.VirtualStaticGroup

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.Group

Multi-valued

No

Required

Yes

Admin Action Required

The Group Implementation must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-http-authorization-mechanism-prop

dsconfig set-http-authorization-mechanism-prop — Modifies HTTP Authorization Mechanism properties

dsconfig set-http-authorization-mechanism-prop

```
dsconfig set-http-authorization-mechanism-prop {options}
```

1 Description

Modifies HTTP Authorization Mechanism properties.

2 Options

The **dsconfig set-http-authorization-mechanism-prop** command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Authorization Mechanism types:

http-anonymous-authorization-mechanism

Default {name}: HTTP Anonymous Authorization Mechanism

Enabled by default: true

See the section called “HTTP Anonymous Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-basic-authorization-mechanism

Default {name}: HTTP Basic Authorization Mechanism

Enabled by default: true

See the section called “HTTP Basic Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-cts-authorization-mechanism

Default {name}: HTTP Oauth2 Cts Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Cts Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-file-authorization-mechanism

Default {name}: HTTP Oauth2 File Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 File Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-openam-authorization-mechanism

Default {name}: HTTP Oauth2 Openam Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Openam Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

http-oauth2-token-introspection-authorization-mechanism

Default {name}: HTTP Oauth2 Token Introspection Authorization Mechanism

Enabled by default: true

See the section called “HTTP Oauth2 Token Introspection Authorization Mechanism” for the properties of this HTTP Authorization Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

HTTP Authorization Mechanism properties depend on the HTTP Authorization Mechanism type, which depends on the `--mechanism-name {name}` option.

3 HTTP Anonymous Authorization Mechanism

HTTP Authorization Mechanisms of type http-anonymous-authorization-mechanism have the following properties:

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

user-dn

Description

The authorization DN which will be used for performing anonymous operations.

Default Value

By default, operations will be performed using an anonymously bound connection.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 HTTP Basic Authorization Mechanism

HTTP Authorization Mechanisms of type http-basic-authorization-mechanism have the following properties:

alt-authentication-enabled

Description

Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-password-header

Description

Alternate HTTP headers to get the user's password from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

alt-username-header

Description

Alternate HTTP headers to get the user's name from.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper used to get the user's entry corresponding to the user-id provided in the HTTP authentication header.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Basic Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 HTTP Oauth2 Cts Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-cts-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Cts Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 HTTP Oauth2 File Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-file-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-directory

Description

Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate.

Default Value

oauth2-demo/

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 File Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

7 HTTP Oauth2 Openam Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-openam-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Openam Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Openam Authorization Mechanism .

Default Value

By default the system key manager(s) will be used.

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-info-url

Description

Defines the OpenAM endpoint URL where the access-token resolution request should be sent.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

8 HTTP Oauth2 Token Introspection Authorization Mechanism

HTTP Authorization Mechanisms of type http-oauth2-token-introspection-authorization-mechanism have the following properties:

access-token-cache-enabled

Description

Indicates whether the HTTP Oauth2 Authorization Mechanism is enabled for use.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

access-token-cache-expiration

Description

Token cache expiration

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

authzid-json-pointer

Description

Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. (example: /uid)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-id

Description

Client's ID to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

client-secret

Description

Client's secret to use during the HTTP basic authentication against the authorization server.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Authorization Mechanism is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

> Specifies the name of the identity mapper to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the HTTP Oauth2 Authorization Mechanism is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the HTTP Oauth2 Token Introspection Authorization Mechanism implementation.

Default Value

org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationM

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.protocols.http.authz.HttpAuthorizationMechanism

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this HTTP Oauth2 Token Introspection Authorization Mechanism .

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent requests to the authorization server.

Advanced Property

No

Read-only

No

required-scope

Description

Scopes required to grant access to the service.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

token-introspection-url

Description

Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect)

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

dsconfig set-http-endpoint-prop

dsconfig set-http-endpoint-prop — Modifies HTTP Endpoint properties

dsconfig set-http-endpoint-prop

```
dsconfig set-http-endpoint-prop {options}
```

1 Description

Modifies HTTP Endpoint properties.

2 Options

The **dsconfig set-http-endpoint-prop** command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following HTTP Endpoint types:

admin-endpoint

Default {name}: Admin Endpoint

Enabled by default: true

See the section called “Admin Endpoint” for the properties of this HTTP Endpoint type.

rest2ldap-endpoint

Default {name}: Rest2ldap Endpoint

Enabled by default: true

See the section called “Rest2ldap Endpoint” for the properties of this HTTP Endpoint type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

HTTP Endpoint properties depend on the HTTP Endpoint type, which depends on the `--endpoint-name {name}` option.

3 Admin Endpoint

HTTP Endpoints of type admin-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.AdminEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Rest2ldap Endpoint

HTTP Endpoints of type rest2ldap-endpoint have the following properties:

authorization-mechanism

Description

The HTTP authorization mechanisms supported by this HTTP Endpoint.

Default Value

None

Allowed Values

The DN of any HTTP Authorization Mechanism. The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-path

Description

All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

config-directory

Description

The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. The directory must be readable by the server and may

contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory.

Default Value

None

Allowed Values

A directory that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the HTTP Endpoint is enabled.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Rest2ldap Endpoint implementation.

Default Value

org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.HttpEndpoint

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-identity-mapper-prop

dsconfig set-identity-mapper-prop — Modifies Identity Mapper properties

dsconfig set-identity-mapper-prop

```
dsconfig set-identity-mapper-prop {options}
```

1 Description

Modifies Identity Mapper properties.

2 Options

The **dsconfig set-identity-mapper-prop** command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

Identity Mapper properties depend on the Identity Mapper type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Identity Mapper types:

exact-match-identity-mapper

Default {name}: Exact Match Identity Mapper

Enabled by default: true

See the section called “Exact Match Identity Mapper” for the properties of this Identity Mapper type.

regular-expression-identity-mapper

Default {name}: Regular Expression Identity Mapper

Enabled by default: true

See the section called “Regular Expression Identity Mapper” for the properties of this Identity Mapper type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Identity Mapper properties depend on the Identity Mapper type, which depends on the `--mapper-name {name}` option.

3 Exact Match Identity Mapper

Identity Mappers of type exact-match-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation.

Default Value

org.opends.server.extensions.ExactMatchIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the set of base DNs below which to search for users. The base DNs will be used when performing searches to map the provided

ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Regular Expression Identity Mapper

Identity Mappers of type regular-expression-identity-mapper have the following properties:

enabled

Description

Indicates whether the Identity Mapper is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation.

Default Value

org.opends.server.extensions.RegularExpressionIdentityMapper

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.IdentityMapper

Multi-valued

No

Required

Yes

Admin Action Required

The Identity Mapper must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry.

Default Value

uid

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

match-base-dn

Description

Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs.

Default Value

The server searches below all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

match-pattern

Description

Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups.

Default Value

None

Allowed Values

Any valid regular expression pattern which is supported by the javax.util.regex.Pattern class (see http://download.oracle.com/docs/

cd/E17409_01/javase/6/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 6).

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replace-pattern

Description

Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used.

Default Value

The replace pattern will be the empty string.

Allowed Values

Any valid replacement string that is allowed by the javax.util.regex.Matcher class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-key-manager-provider-prop

dsconfig set-key-manager-provider-prop — Modifies Key Manager Provider properties

dsconfig set-key-manager-provider-prop

`dsconfig set-key-manager-provider-prop {options}`

1 Description

Modifies Key Manager Provider properties.

2 Options

The **dsconfig set-key-manager-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Key Manager Provider.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Key Manager Provider types:

file-based-key-manager-provider

Default {name}: File Based Key Manager Provider

Enabled by default: true

See the section called “File Based Key Manager Provider” for the properties of this Key Manager Provider type.

ldap-key-manager-provider

Default {name}: LDAP Key Manager Provider

Enabled by default: true

See the section called “LDAP Key Manager Provider” for the properties of this Key Manager Provider type.

pkcs11-key-manager-provider

Default {name}: PKCS11 Key Manager Provider

Enabled by default: true

See the section called “PKCS11 Key Manager Provider” for the properties of this Key Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Key Manager Provider properties depend on the Key Manager Provider type, which depends on the `--provider-name {name}` option.

3 File Based Key Manager Provider

Key Manager Providers of type file-based-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-type

Description

Specifies the format for the data in the key store file. Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 LDAP Key Manager Provider

Key Manager Providers of type ldap-key-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPKeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

5 PKCS11 Key Manager Provider

Key Manager Providers of type pkcs11-key-manager-provider have the following properties:

enabled

Description

Indicates whether the Key Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Key Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11KeyManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.KeyManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Key Manager Provider must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined environment variable that contains the clear-text PIN required to access the contents of the key store.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

key-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Key Manager Provider .

Default Value

None

Allowed Values

The name of a defined Java property.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Key Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig set-log-publisher-prop

dsconfig set-log-publisher-prop — Modifies Log Publisher properties

dsconfig set-log-publisher-prop

```
dsconfig set-log-publisher-prop {options}
```

1 Description

Modifies Log Publisher properties.

2 Options

The **dsconfig set-log-publisher-prop** command takes the following options:

`--publisher-name {name}`

The name of the Log Publisher.

Log Publisher properties depend on the Log Publisher type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Publisher types:

csv-file-access-log-publisher

Default {name}: Csv File Access Log Publisher

Enabled by default: true

See the section called “Csv File Access Log Publisher” for the properties of this Log Publisher type.

csv-file-http-access-log-publisher

Default {name}: Csv File HTTP Access Log Publisher

Enabled by default: true

See the section called “Csv File HTTP Access Log Publisher” for the properties of this Log Publisher type.

external-access-log-publisher

Default {name}: External Access Log Publisher

Enabled by default: true

See the section called “External Access Log Publisher” for the properties of this Log Publisher type.

external-http-access-log-publisher

Default {name}: External HTTP Access Log Publisher

Enabled by default: true

See the section called “External HTTP Access Log Publisher” for the properties of this Log Publisher type.

file-based-access-log-publisher

Default {name}: File Based Access Log Publisher

Enabled by default: true

See the section called “File Based Access Log Publisher” for the properties of this Log Publisher type.

file-based-audit-log-publisher

Default {name}: File Based Audit Log Publisher

Enabled by default: true

See the section called “File Based Audit Log Publisher” for the properties of this Log Publisher type.

file-based-debug-log-publisher

Default {name}: File Based Debug Log Publisher

Enabled by default: true

See the section called “File Based Debug Log Publisher” for the properties of this Log Publisher type.

file-based-error-log-publisher

Default {name}: File Based Error Log Publisher

Enabled by default: true

See the section called “File Based Error Log Publisher” for the properties of this Log Publisher type.

file-based-http-access-log-publisher

Default {name}: File Based HTTP Access Log Publisher

Enabled by default: true

See the section called “File Based HTTP Access Log Publisher” for the properties of this Log Publisher type.

json-file-access-log-publisher

Default {name}: Json File Access Log Publisher

Enabled by default: true

See the section called “Json File Access Log Publisher” for the properties of this Log Publisher type.

json-file-http-access-log-publisher

Default {name}: Json File HTTP Access Log Publisher

Enabled by default: true

See the section called “Json File HTTP Access Log Publisher” for the properties of this Log Publisher type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Log Publisher properties depend on the Log Publisher type, which depends on the `--publisher-name {name}` option.

3 Csv File Access Log Publisher

Log Publishers of type csv-file-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writting in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CsvFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when the tamper-evident option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Csv File HTTP Access Log Publisher

Log Publishers of type csv-file-http-access-log-publisher have the following properties:

asynchronous

Description

Indicates whether the Csv File HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-delimiter-char

Description

The delimiter character to use when writing in CSV format.

Default Value

,

Allowed Values

The delimiter character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

csv-eol-symbols

Description

The string that marks the end of a line.

Default Value

Use the platform specific end of line character sequence.

Allowed Values

The string that marks the end of a line.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

csv-quote-char

Description

The character to append and prepend to a CSV field when writing in CSV format.

Default Value

"

Allowed Values

The quote character to use when writing in CSV format.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Csv File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-store-file

Description

Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. Changes to this property will take effect the next time that the key store is accessed.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

key-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the Csv File HTTP Access Log Publisher .

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the Csv File HTTP Access Log Publisher is accessed.

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Csv File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Csv File HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

signature-time-interval

Description

Specifies the interval at which to sign the log file when secure option is enabled.

Default Value

3s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

tamper-evident

Description

Specifies whether the log should be signed in order to detect tampering. Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 External Access Log Publisher

Log Publishers of type external-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External Access Log Publisher implementation.

Default Value

org.opends.server.loggers.ExternalAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 External HTTP Access Log Publisher

Log Publishers of type external-http-access-log-publisher have the following properties:

config-file

Description

The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 File Based Access Log Publisher

Log Publishers of type file-based-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the access log.

Default Value

multi-line

Allowed Values

combined

Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).

multi-line

Outputs separate log records for operation requests and responses.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 File Based Audit Log Publisher

Log Publishers of type file-based-audit-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Audit Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation.

Default Value

org.opends.server.loggers.TextAuditLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Audit Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Audit Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Audit Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 File Based Debug Log Publisher

Log Publishers of type file-based-debug-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Debug Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-debug-exceptions-only

Description

Indicates whether only logs with exception should be logged.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-include-throwable-cause

Description

Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-entry-arguments

Description

Indicates whether to include method arguments in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-omit-method-return-value

Description

Indicates whether to include the return value in debug messages logged by default.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-throwable-stack-frames

Description

Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages.

Default Value

2147483647

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation.

Default Value

org.opends.server.loggers.TextDebugLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Debug Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Debug Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Debug Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Debug Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds

- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 File Based Error Log Publisher

Log Publishers of type file-based-error-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based Error Log Publisher will publish records asynchronously.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

default-severity

Description

Specifies the default severity levels for the logger.

Default Value

error

warning

Allowed Values

all

Messages of all severity levels are logged.

debug

The error log severity that is used for messages that provide debugging information triggered during processing.

error

The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.

info

The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.

none

No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.

notice

The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).

warning

The error log severity that is used for messages that provide information about warnings triggered during processing.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation.

Default Value

org.opends.server.loggers.TextErrorLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based Error Log Publisher . The path to the file is relative to the server root.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based Error Log Publisher .

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

override-severity

Description

Specifies the override severity levels for the logger based on the category of the messages. Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control,

admin, sync, version, quicksetup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug.

Default Value

All messages with the default severity levels are logged.

Allowed Values

A string in the form category=severity1,severity2...

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based Error Log Publisher . When multiple policies are used, log files will be cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files will never be cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based Error Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

11 File Based HTTP Access Log Publisher

Log Publishers of type file-based-http-access-log-publisher have the following properties:

append

Description

Specifies whether to append to existing log files.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

asynchronous

Description

Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

auto-flush

Description

Specifies whether to flush the writer after every log record. If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

buffer-size

Description

Specifies the log file buffer size.

Default Value

64kb

Allowed Values

Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.TextHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root.

Default Value

None

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

log-file-permissions

Description

The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher.

Default Value

640

Allowed Values

A valid UNIX mode string. The mode string must contain three digits between zero and seven.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

log-format

Description

Specifies how log records should be formatted and written to the HTTP access log.

Default Value

cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id

Allowed Values

A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true OpenDJ

supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-record-time-format

Description

Specifies the format string that is used to generate log record timestamps.

Default Value

dd/MMM/yyyy:HH:mm:ss Z

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

The maximum number of log records that can be stored in the asynchronous queue.

Default Value

5000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

retention-policy

Description

The retention policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the File Based HTTP Access Log Publisher . When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

time-interval

Description

Specifies the interval at which to check whether the log files need to be rotated.

Default Value

5s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

12 Json File Access Log Publisher

Log Publishers of type json-file-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filtering-policy

Description

Specifies how filtering criteria should be applied to log records.

Default Value

no-filtering

Allowed Values

exclusive

Records must not match any of the filtering criteria in order to be logged.

inclusive

Records must match at least one of the filtering criteria in order to be logged.

no-filtering

No filtering will be performed, and all records will be logged.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File Access Log Publisher implementation.

Default Value

org.opends.server.loggers.JsonFileAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-control-oids

Description

Specifies whether control OIDs will be included in operation log records.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

suppress-internal-operations

Description

Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

suppress-synchronization-operations

Description

Indicates whether access messages that are generated by synchronization operations should be suppressed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 Json File HTTP Access Log Publisher

Log Publishers of type json-file-http-access-log-publisher have the following properties:

enabled

Description

Indicates whether the Log Publisher is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Json File HTTP Access Log Publisher implementation.

Default Value

org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.LogPublisher

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-directory

Description

The directory to use for the log files generated by the Json File HTTP Access Log Publisher. The path to the directory is relative to the server root.

Default Value

logs

Allowed Values

A path to an existing directory that is readable and writable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

The Log Publisher must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

retention-policy

Description

The retention policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, log files are cleaned when any of the policy's conditions are met.

Default Value

No retention policy is used and log files are never cleaned.

Allowed Values

The DN of any Log Retention Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rotation-policy

Description

The rotation policy to use for the Json File HTTP Access Log Publisher. When multiple policies are used, rotation will occur if any policy's conditions are met.

Default Value

No rotation policy is used and log rotation will not occur.

Allowed Values

The DN of any Log Rotation Policy.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-log-retention-policy-prop

dsconfig set-log-retention-policy-prop — Modifies Log Retention Policy properties

dsconfig set-log-retention-policy-prop

```
dsconfig set-log-retention-policy-prop {options}
```

1 Description

Modifies Log Retention Policy properties.

2 Options

The **dsconfig set-log-retention-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Retention Policy types:

file-count-log-retention-policy

Default {name}: File Count Log Retention Policy

Enabled by default: false

See the section called “File Count Log Retention Policy” for the properties of this Log Retention Policy type.

free-disk-space-log-retention-policy

Default {name}: Free Disk Space Log Retention Policy

Enabled by default: false

See the section called “Free Disk Space Log Retention Policy” for the properties of this Log Retention Policy type.

size-limit-log-retention-policy

Default {name}: Size Limit Log Retention Policy

Enabled by default: false

See the section called “Size Limit Log Retention Policy” for the properties of this Log Retention Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Log Retention Policy properties depend on the Log Retention Policy type, which depends on the `--policy-name {name}` option.

3 File Count Log Retention Policy

Log Retention Policies of type file-count-log-retention-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FileNumberRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

number-of-files

Description

Specifies the number of archived log files to retain before the oldest ones are cleaned.

Default Value

None

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Free Disk Space Log Retention Policy

Log Retention Policies of type free-disk-space-log-retention-policy have the following properties:

free-disk-space

Description

Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation.

Default Value

org.opends.server.loggers.FreeDiskSpaceRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Size Limit Log Retention Policy

Log Retention Policies of type size-limit-log-retention-policy have the following properties:

disk-space-used

Description

Specifies the maximum total disk space used by the log files.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRetentionPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RetentionPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-log-rotation-policy-prop

dsconfig set-log-rotation-policy-prop — Modifies Log Rotation Policy properties

dsconfig set-log-rotation-policy-prop

```
dsconfig set-log-rotation-policy-prop {options}
```

1 Description

Modifies Log Rotation Policy properties.

2 Options

The **dsconfig set-log-rotation-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Log Rotation Policy types:

fixed-time-log-rotation-policy

Default {name}: Fixed Time Log Rotation Policy

Enabled by default: false

See the section called “Fixed Time Log Rotation Policy” for the properties of this Log Rotation Policy type.

size-limit-log-rotation-policy

Default {name}: Size Limit Log Rotation Policy

Enabled by default: false

See the section called “Size Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

time-limit-log-rotation-policy

Default {name}: Time Limit Log Rotation Policy

Enabled by default: false

See the section called “Time Limit Log Rotation Policy” for the properties of this Log Rotation Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Log Rotation Policy properties depend on the Log Rotation Policy type, which depends on the `--policy-name {name}` option.

3 Fixed Time Log Rotation Policy

Log Rotation Policies of type fixed-time-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.FixedTimeRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

time-of-day

Description

Specifies the time of day at which log rotation should occur.

Default Value

None

Allowed Values

24 hour time of day in HHmm format.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Size Limit Log Rotation Policy

Log Rotation Policies of type size-limit-log-rotation-policy have the following properties:

file-size-limit

Description

Specifies the maximum size that a log file can reach before it is rotated.

Default Value

None

Allowed Values

Lower value is 1.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.SizeBasedRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Time Limit Log Rotation Policy

Log Rotation Policies of type time-limit-log-rotation-policy have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation.

Default Value

org.opends.server.loggers.TimeLimitRotationPolicy

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.loggers.RotationPolicy

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

rotation-interval

Description

Specifies the time interval between rotations.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours

- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-monitor-provider-prop

dsconfig set-monitor-provider-prop — Modifies Monitor Provider properties

dsconfig set-monitor-provider-prop

```
dsconfig set-monitor-provider-prop {options}
```

1 Description

Modifies Monitor Provider properties.

2 Options

The **dsconfig set-monitor-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Monitor Provider.

Monitor Provider properties depend on the Monitor Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Monitor Provider types:

client-connection-monitor-provider

Default {name}: Client Connection Monitor Provider

Enabled by default: true

See the section called “Client Connection Monitor Provider” for the properties of this Monitor Provider type.

entry-cache-monitor-provider

Default {name}: Entry Cache Monitor Provider

Enabled by default: true

See the section called “Entry Cache Monitor Provider” for the properties of this Monitor Provider type.

memory-usage-monitor-provider

Default {name}: Memory Usage Monitor Provider

Enabled by default: true

See the section called “Memory Usage Monitor Provider” for the properties of this Monitor Provider type.

stack-trace-monitor-provider

Default {name}: Stack Trace Monitor Provider

Enabled by default: true

See the section called “Stack Trace Monitor Provider” for the properties of this Monitor Provider type.

system-info-monitor-provider

Default {name}: System Info Monitor Provider

Enabled by default: true

See the section called “System Info Monitor Provider” for the properties of this Monitor Provider type.

version-monitor-provider

Default {name}: Version Monitor Provider

Enabled by default: true

See the section called “Version Monitor Provider” for the properties of this Monitor Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Monitor Provider properties depend on the Monitor Provider type, which depends on the `--provider-name {name}` option.

3 Client Connection Monitor Provider

Monitor Providers of type client-connection-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Client Connection Monitor Provider implementation.

Default Value

org.opends.server.monitors.ClientConnectionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Entry Cache Monitor Provider

Monitor Providers of type entry-cache-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Entry Cache Monitor Provider implementation.

Default Value

org.opends.server.monitors.EntryCacheMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Memory Usage Monitor Provider

Monitor Providers of type memory-usage-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Memory Usage Monitor Provider implementation.

Default Value

org.opends.server.monitors.MemoryUsageMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Stack Trace Monitor Provider

Monitor Providers of type stack-trace-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Stack Trace Monitor Provider implementation.

Default Value

org.opends.server.monitors.StackTraceMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 System Info Monitor Provider

Monitor Providers of type system-info-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the System Info Monitor Provider implementation.

Default Value

org.opends.server.monitors.SystemInfoMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Version Monitor Provider

Monitor Providers of type version-monitor-provider have the following properties:

enabled

Description

Indicates whether the Monitor Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Version Monitor Provider implementation.

Default Value

org.opends.server.monitors.VersionMonitorProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.MonitorProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-password-generator-prop

dsconfig set-password-generator-prop — Modifies Password Generator properties

dsconfig set-password-generator-prop

```
dsconfig set-password-generator-prop {options}
```

1 Description

Modifies Password Generator properties.

2 Options

The **dsconfig set-password-generator-prop** command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

Password Generator properties depend on the Password Generator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Generator types:

random-password-generator

Default {name}: Random Password Generator

Enabled by default: true

See the section called “Random Password Generator” for the properties of this Password Generator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Password Generator properties depend on the Password Generator type, which depends on the `--generator-name {name}` option.

3 Random Password Generator

Password Generators of type random-password-generator have the following properties:

enabled

Description

Indicates whether the Password Generator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation.

Default Value

org.opends.server.extensions.RandomPasswordGenerator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordGenerator

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

password-character-set

Description

Specifies one or more named character sets. This is a multi-valued property, with each value defining a different character set. The

format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters.

Default Value

None

Allowed Values

A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-format

Description

Specifies the format to use for the generated password. The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set.

Default Value

None

Allowed Values

A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-password-policy-prop

dsconfig set-password-policy-prop — Modifies Authentication Policy properties

dsconfig set-password-policy-prop

```
dsconfig set-password-policy-prop {options}
```

1 Description

Modifies Authentication Policy properties.

2 Options

The **dsconfig set-password-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

Authentication Policy properties depend on the Authentication Policy type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Authentication Policy types:

ldap-pass-through-authentication-policy

Default {name}: LDAP Pass Through Authentication Policy

Enabled by default: false

See the section called “LDAP Pass Through Authentication Policy” for the properties of this Authentication Policy type.

password-policy

Default {name}: Password Policy

Enabled by default: false

See the section called “Password Policy” for the properties of this Authentication Policy type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Authentication Policy properties depend on the Authentication Policy type, which depends on the `--policy-name {name}` option.

3 LDAP Pass Through Authentication Policy

Authentication Policies of type ldap-pass-through-authentication-policy have the following properties:

cached-password-storage-scheme

Description

Specifies the name of a password storage scheme which should be used for encoding cached passwords. Changing the password storage scheme will cause all existing cached passwords to be discarded.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cached-password-ttl

Description

Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service.

Default Value

8 hours

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds

- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

connection-timeout

Description

Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available.

Default Value

3 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation.

Default Value

org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

mapped-attribute

Description

Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-base-dn

Description

Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. If multiple values are given, searches are performed below all specified base DNs.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-dn

Description

Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service.

Default Value

Searches will be performed anonymously.

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password

Description

Specifies the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-environment-variable

Description

Specifies the name of an environment variable containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-file

Description

Specifies the name of a file containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-bind-password-property

Description

Specifies the name of a Java property containing the bind password which should be used to perform user searches in the remote LDAP directory service.

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapped-search-filter-template

Description

If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "(&(uid=%s)(objectclass=student))"

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

mapping-policy

Description

Specifies the mapping algorithm for obtaining the bind DN from the user's entry.

Default Value

unmapped

Allowed Values

mapped-bind

Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.

mapped-search

Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then the filter will be composed of multiple equality filters combined using a logical OR (union).

unmapped

Bind to the remote LDAP directory service using the DN of the user's entry in this directory server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

primary-remote-ldap-server

Description

Specifies the primary list of remote LDAP servers which should be used for pass through authentication. If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-remote-ldap-server

Description

Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available.

Default Value

No secondary LDAP servers.

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cipher-suite

Description

Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL cipher suites provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

ssl-protocol

Description

Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections.

Default Value

Uses the default set of SSL protocols provided by the server's JVM.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change.

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers.

Default Value

By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when SSL is enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations.

Advanced Property

No

Read-only

No

use-password-caching

Description

Indicates whether passwords should be cached locally within the user's entry.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the LDAP Pass Through Authentication Policy should use SSL. If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-tcp-keep-alive

Description

Indicates whether LDAP connections should use TCP keep-alive. If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

use-tcp-no-delay

Description

Indicates whether LDAP connections should use TCP no-delay. If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Password Policy

Authentication Policies of type password-policy have the following properties:

account-status-notification-handler

Description

Specifies the names of the account status notification handlers that are used with the associated password storage scheme.

Default Value

None

Allowed Values

The DN of any Account Status Notification Handler. The referenced account status notification handlers must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-expired-password-changes

Description

Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

allow-multiple-password-values

Description

Indicates whether user entries can have multiple distinct values for the password attribute. This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-pre-encoded-passwords

Description

Indicates whether users can change their passwords by providing a pre-encoded value. This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-user-password-changes

Description

Indicates whether users can change their own passwords. This check is made in addition to access control evaluation. Both must allow the password change for it to occur.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-password-storage-scheme

Description

Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy.

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

deprecated-password-storage-scheme

Description

Specifies the names of the password storage schemes that are considered deprecated for this password policy. If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s).

Default Value

None

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

expire-passwords-without-warning

Description

Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-add

Description

Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

force-change-on-reset

Description

Indicates whether users are forced to change their passwords if they are reset by an administrator. For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

grace-login-count

Description

Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. A value of 0 indicates that no grace logins are allowed.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

idle-lockout-interval

Description

Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class which provides the Password Policy implementation.

Default Value

org.opends.server.core.PasswordPolicyFactory

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.AuthenticationPolicyFactory

Multi-valued

No

Required

Yes

Admin Action Required

The Authentication Policy must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

last-login-time-attribute

Description

Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

last-login-time-format

Description

Specifies the format string that is used to generate the last login time value for users with the associated password policy. This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-duration

Description

Specifies the length of time that an account is locked after too many authentication failures. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-count

Description

Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. A value of 0 indicates that accounts are never locked out due to failed attempts.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

lockout-failure-expiration-interval

Description

Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds indicates that the authentication failures must never expire. The failure count is always cleared upon a successful authentication.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-age

Description

Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables password expiration.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

max-password-reset-age

Description

Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables this feature.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-age

Description

Specifies the minimum length of time after a password change before the user is allowed to change the password again. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or

weeks. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-attribute

Description

Specifies the attribute type used to hold user passwords. This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

password-change-requires-current-password

Description

Indicates whether user password changes must use the password modify extended operation and must include the user's current password before the change is allowed.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-expiration-warning-interval

Description

Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, or weeks. A value of 0 seconds disables the warning interval.

Default Value

5 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-generator

Description

Specifies the name of the password generator that is used with the associated password policy. This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request.

Default Value

None

Allowed Values

The DN of any Password Generator. The referenced password generator must be enabled.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-count

Description

Specifies the maximum number of former passwords to maintain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds).

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-history-duration

Description

Specifies the maximum length of time that passwords remain in the password history. When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero).

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.Upper limit is 2147483647 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

password-validator

Description

Specifies the names of the password validators that are used with the associated password storage scheme. The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable.

Default Value

None

Allowed Values

The DN of any Password Validator. The referenced password validators must be enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

previous-last-login-time-format

Description

Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class.

Default Value

None

Allowed Values

Any valid format string that can be used with the java.text.SimpleDateFormat class.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-change-by-time

Description

Specifies the time by which all users with the associated password policy must change their passwords. The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset.

Default Value

None

Allowed Values

A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT).

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-authentication

Description

Indicates whether users with the associated password policy are required to authenticate in a secure manner. This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

require-secure-password-changes

Description

Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

skip-validation-for-administrators

Description

Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

state-update-failure-policy

Description

Specifies how the server deals with the inability to update password policy state information during an authentication attempt. In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password

policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled).

Default Value

reactive

Allowed Values

ignore

If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user.

proactive

Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.

reactive

Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-password-storage-scheme-prop

dsconfig set-password-storage-scheme-prop — Modifies Password Storage Scheme properties

dsconfig set-password-storage-scheme-prop

```
dsconfig set-password-storage-scheme-prop {options}
```

1 Description

Modifies Password Storage Scheme properties.

2 Options

The **dsconfig set-password-storage-scheme-prop** command takes the following options:

`--scheme-name {name}`

The name of the Password Storage Scheme.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Storage Scheme types:

aes-password-storage-scheme

Default {name}: AES Password Storage Scheme

Enabled by default: true

See the section called “AES Password Storage Scheme” for the properties of this Password Storage Scheme type.

base64-password-storage-scheme

Default {name}: Base64 Password Storage Scheme

Enabled by default: true

See the section called “Base64 Password Storage Scheme” for the properties of this Password Storage Scheme type.

bcrypt-password-storage-scheme

Default {name}: Bcrypt Password Storage Scheme

Enabled by default: true

See the section called “Bcrypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

blowfish-password-storage-scheme

Default {name}: Blowfish Password Storage Scheme

Enabled by default: true

See the section called “Blowfish Password Storage Scheme” for the properties of this Password Storage Scheme type.

clear-password-storage-scheme

Default {name}: Clear Password Storage Scheme

Enabled by default: true

See the section called “Clear Password Storage Scheme” for the properties of this Password Storage Scheme type.

crypt-password-storage-scheme

Default {name}: Crypt Password Storage Scheme

Enabled by default: true

See the section called “Crypt Password Storage Scheme” for the properties of this Password Storage Scheme type.

md5-password-storage-scheme

Default {name}: MD5 Password Storage Scheme

Enabled by default: true

See the section called “MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha256-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA256 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pbkdf2-hmac-sha512-password-storage-scheme

Default {name}: PBKDF2 Hmac SHA512 Password Storage Scheme

Enabled by default: true

See the section called “PBKDF2 Hmac SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

pkcs5s2-password-storage-scheme

Default {name}: PKCS5S2 Password Storage Scheme

Enabled by default: true

See the section called “PKCS5S2 Password Storage Scheme” for the properties of this Password Storage Scheme type.

rc4-password-storage-scheme

Default {name}: RC4 Password Storage Scheme

Enabled by default: true

See the section called “RC4 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-md5-password-storage-scheme

Default {name}: Salted MD5 Password Storage Scheme

Enabled by default: true

See the section called “Salted MD5 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha1-password-storage-scheme

Default {name}: Salted SHA1 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha256-password-storage-scheme

Default {name}: Salted SHA256 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA256 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha384-password-storage-scheme

Default {name}: Salted SHA384 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA384 Password Storage Scheme” for the properties of this Password Storage Scheme type.

salted-sha512-password-storage-scheme

Default {name}: Salted SHA512 Password Storage Scheme

Enabled by default: true

See the section called “Salted SHA512 Password Storage Scheme” for the properties of this Password Storage Scheme type.

sha1-password-storage-scheme

Default {name}: SHA1 Password Storage Scheme

Enabled by default: true

See the section called “SHA1 Password Storage Scheme” for the properties of this Password Storage Scheme type.

triple-des-password-storage-scheme

Default {name}: Triple DES Password Storage Scheme

Enabled by default: true

See the section called “Triple DES Password Storage Scheme” for the properties of this Password Storage Scheme type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Password Storage Scheme properties depend on the Password Storage Scheme type, which depends on the `--scheme-name {name}` option.

3 AES Password Storage Scheme

Password Storage Schemes of type aes-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.AESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Base64 Password Storage Scheme

Password Storage Schemes of type base64-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.Base64PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Bcrypt Password Storage Scheme

Password Storage Schemes of type bcrypt-password-storage-scheme have the following properties:

bcrypt-cost

Description

The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users.

Default Value

12

Allowed Values

An integer value. Lower value is 1. Upper value is 30.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BcryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Blowfish Password Storage Scheme

Password Storage Schemes of type blowfish-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.BlowfishPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 Clear Password Storage Scheme

Password Storage Schemes of type clear-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.ClearPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 Crypt Password Storage Scheme

Password Storage Schemes of type crypt-password-storage-scheme have the following properties:

crypt-password-storage-encryption-algorithm

Description

Specifies the algorithm to use to encrypt new passwords. Select the crypt algorithm to use to encrypt new passwords. The value can either be

"unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a 1 prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a 5 prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a 6 prefix.

Default Value

unix

Allowed Values

md5

New passwords are encrypted with the BSD MD5 algorithm.

sha256

New passwords are encrypted with the Unix crypt SHA256 algorithm.

sha512

New passwords are encrypted with the Unix crypt SHA512 algorithm.

unix

New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.CryptPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 MD5 Password Storage Scheme

Password Storage Schemes of type md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.MD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 PBKDF2 Hmac SHA256 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 PBKDF2 Hmac SHA512 Password Storage Scheme

Password Storage Schemes of type pbkdf2-hmac-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PBKDF2 Hmac SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pbkdf2-iterations

Description

The number of algorithm iterations to make. NIST recommends at least 1000.

Default Value

10000

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 PKCS5S2 Password Storage Scheme

Password Storage Schemes of type pkcs5s2-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the PKCS5S2 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.PKCS5S2PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

13 RC4 Password Storage Scheme

Password Storage Schemes of type rc4-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.RC4PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Salted MD5 Password Storage Scheme

Password Storage Schemes of type salted-md5-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedMD5PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

15 Salted SHA1 Password Storage Scheme

Password Storage Schemes of type salted-sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

16 Salted SHA256 Password Storage Scheme

Password Storage Schemes of type salted-sha256-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA256 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA256PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

17 Salted SHA384 Password Storage Scheme

Password Storage Schemes of type salted-sha384-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA384 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA384PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

18 Salted SHA512 Password Storage Scheme

Password Storage Schemes of type salted-sha512-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Salted SHA512 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SaltedSHA512PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

19 SHA1 Password Storage Scheme

Password Storage Schemes of type sha1-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SHA1 Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.SHA1PasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

20 Triple DES Password Storage Scheme

Password Storage Schemes of type triple-des-password-storage-scheme have the following properties:

enabled

Description

Indicates whether the Password Storage Scheme is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Triple DES Password Storage Scheme implementation.

Default Value

org.opends.server.extensions.TripleDESPasswordStorageScheme

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordStorageScheme

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-password-validator-prop

dsconfig set-password-validator-prop — Modifies Password Validator properties

dsconfig set-password-validator-prop

`dsconfig set-password-validator-prop {options}`

1 Description

Modifies Password Validator properties.

2 Options

The **dsconfig set-password-validator-prop** command takes the following options:

`--validator-name {name}`

The name of the Password Validator.

Password Validator properties depend on the Password Validator type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Password Validator types:

attribute-value-password-validator

Default {name}: Attribute Value Password Validator

Enabled by default: true

See the section called “Attribute Value Password Validator” for the properties of this Password Validator type.

character-set-password-validator

Default {name}: Character Set Password Validator

Enabled by default: true

See the section called “Character Set Password Validator” for the properties of this Password Validator type.

dictionary-password-validator

Default {name}: Dictionary Password Validator

Enabled by default: true

See the section called “Dictionary Password Validator” for the properties of this Password Validator type.

length-based-password-validator

Default {name}: Length Based Password Validator

Enabled by default: true

See the section called “Length Based Password Validator” for the properties of this Password Validator type.

repeated-characters-password-validator

Default {name}: Repeated Characters Password Validator

Enabled by default: true

See the section called “Repeated Characters Password Validator” for the properties of this Password Validator type.

similarity-based-password-validator

Default {name}: Similarity Based Password Validator

Enabled by default: true

See the section called “Similarity Based Password Validator” for the properties of this Password Validator type.

unique-characters-password-validator

Default {name}: Unique Characters Password Validator

Enabled by default: true

See the section called “Unique Characters Password Validator” for the properties of this Password Validator type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Password Validator properties depend on the Password Validator type, which depends on the `--validator-name {name}` option.

3 Attribute Value Password Validator

Password Validators of type attribute-value-password-validator have the following properties:

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against attribute values. If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.AttributeValuePasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

match-attribute

Description

Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry.

Default Value

All attributes in the user entry will be checked.

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Character Set Password Validator

Password Validators of type character-set-password-validator have the following properties:

allow-unclassified-characters

Description

Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set

Description

Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters

required from that set. Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set.

Default Value

If no sets are specified, the validator only uses the defined character ranges.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

character-set-ranges

Description

Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For

example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered.

Default Value

If no ranges are specified, the validator only uses the defined character sets.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.CharacterSetPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-character-sets

Description

Specifies the minimum number of character sets and ranges that a password must contain. This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3.

Default Value

The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Dictionary Password Validator

Password Validators of type dictionary-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator is to treat password characters in a case-sensitive manner. If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

check-substrings

Description

Indicates whether this password validator is to match portions of the password string against dictionary words. If "false" then only match the entire password against words otherwise ("true") check whether the password contains words.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dictionary-file

Description

Specifies the path to the file containing a list of words that cannot be used as passwords. It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root.

Default Value

For Unix and Linux systems: config/wordlist.txt. For Windows systems: config\wordlist.txt

Allowed Values

The path to any text file contained on the system that is readable by the server.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.DictionaryPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-substring-length

Description

Indicates the minimal length of the substring within the password in case substring checking is enabled. If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords.

Default Value

5

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

test-reversed-password

Description

Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Length Based Password Validator

Password Validators of type length-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.LengthBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-password-length

Description

Specifies the maximum number of characters that can be included in a proposed password. A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

0

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

min-password-length

Description

Specifies the minimum number of characters that must be included in a proposed password. A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length.

Default Value

6

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Repeated Characters Password Validator

Password Validators of type repeated-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.RepeatedCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-consecutive-length

Description

Specifies the maximum number of times that any character can appear consecutively in a password value. A value of zero indicates that no maximum limit is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Similarity Based Password Validator

Password Validators of type similarity-based-password-validator have the following properties:

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.SimilarityBasedPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-password-difference

Description

Specifies the minimum difference of new and old password. A value of zero indicates that no difference between passwords is acceptable.

Default Value

None

Allowed Values

An integer value. Lower value is 0. Upper value is 2147483647.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Unique Characters Password Validator

Password Validators of type unique-characters-password-validator have the following properties:

case-sensitive-validation

Description

Indicates whether this password validator should treat password characters in a case-sensitive manner. A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the password validator is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the password validator implementation.

Default Value

org.opends.server.extensions.UniqueCharactersPasswordValidator

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.PasswordValidator

Multi-valued

No

Required

Yes

Admin Action Required

The Password Validator must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

min-unique-characters

Description

Specifies the minimum number of unique characters that a password will be allowed to contain. A value of zero indicates that no minimum value is enforced.

Default Value

None

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-plugin-prop

dsconfig set-plugin-prop — Modifies Plugin properties

dsconfig set-plugin-prop

```
dsconfig set-plugin-prop {options}
```

1 Description

Modifies Plugin properties.

2 Options

The **dsconfig set-plugin-prop** command takes the following options:

`--plugin-name {name}`

The name of the Plugin.

Plugin properties depend on the Plugin type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Plugin types:

attribute-cleanup-plugin

Default {name}: Attribute Cleanup Plugin

Enabled by default: true

See the section called “Attribute Cleanup Plugin” for the properties of this Plugin type.

change-number-control-plugin

Default {name}: Change Number Control Plugin

Enabled by default: true

See the section called “Change Number Control Plugin” for the properties of this Plugin type.

entry-uuid-plugin

Default {name}: Entry UUID Plugin

Enabled by default: true

See the section called “Entry UUID Plugin” for the properties of this Plugin type.

fractional-ldif-import-plugin

Default {name}: Fractional LDIF Import Plugin

Enabled by default: true

See the section called “Fractional LDIF Import Plugin” for the properties of this Plugin type.

last-mod-plugin

Default {name}: Last Mod Plugin

Enabled by default: true

See the section called “Last Mod Plugin” for the properties of this Plugin type.

ldap-attribute-description-list-plugin

Default {name}: LDAP Attribute Description List Plugin

Enabled by default: true

See the section called “LDAP Attribute Description List Plugin” for the properties of this Plugin type.

password-policy-import-plugin

Default {name}: Password Policy Import Plugin

Enabled by default: true

See the section called “Password Policy Import Plugin” for the properties of this Plugin type.

profiler-plugin

Default {name}: Profiler Plugin

Enabled by default: true

See the section called “Profiler Plugin” for the properties of this Plugin type.

referential-integrity-plugin

Default {name}: Referential Integrity Plugin

Enabled by default: true

See the section called “Referential Integrity Plugin” for the properties of this Plugin type.

samba-password-plugin

Default {name}: Samba Password Plugin

Enabled by default: true

See the section called “Samba Password Plugin” for the properties of this Plugin type.

seven-bit-clean-plugin

Default {name}: Seven Bit Clean Plugin

Enabled by default: true

See the section called “Seven Bit Clean Plugin” for the properties of this Plugin type.

unique-attribute-plugin

Default {name}: Unique Attribute Plugin

Enabled by default: true

See the section called “Unique Attribute Plugin” for the properties of this Plugin type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Plugin properties depend on the Plugin type, which depends on the `--plugin-name {name}` option.

3 Attribute Cleanup Plugin

Plugins of type attribute-cleanup-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.AttributeCleanupPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparseadd

preparsemodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

remove-inbound-attributes

Description

A list of attributes which should be removed from incoming add or modify requests.

Default Value

No attributes will be removed

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

rename-inbound-attributes

Description

A list of attributes which should be renamed in incoming add or modify requests.

Default Value

No attributes will be renamed

Allowed Values

An attribute name mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Change Number Control Plugin

Plugins of type change-number-control-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that

it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ChangeNumberControlPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postOperationAdd

postOperationDelete

postOperationModify

postOperationModifyDN

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Entry UUID Plugin

Plugins of type entry-uuid-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.EntryUUIDPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preoperationadd

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

6 Fractional LDIF Import Plugin

Plugins of type fractional-ldif-import-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

None

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

None

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

7 Last Mod Plugin

Plugins of type last-mod-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that

it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LastModPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

8 LDAP Attribute Description List Plugin

Plugins of type ldap-attribute-description-list-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.LDAPADListPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preparsesearch

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

9 Password Policy Import Plugin

Plugins of type password-policy-import-plugin have the following properties:

default-auth-password-storage-scheme

Description

Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them.

Default Value

If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

default-user-password-storage-scheme

Description

Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password

syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them.

Default Value

If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme.

Allowed Values

The DN of any Password Storage Scheme. The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.PasswordPolicyImportPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

10 Profiler Plugin

Plugins of type profiler-plugin have the following properties:

enable-profiling-on-startup

Description

Indicates whether the profiler plug-in is to start collecting data automatically when the directory server is started. This property is read only when the server is started, and any changes take effect on the next restart. This property is typically set to "false" unless startup profiling is required, because otherwise the volume of data that can be collected can cause the server to run out of memory if it is not turned off in a timely manner.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.profiler.ProfilerPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

startup

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

profile-action

Description

Specifies the action that should be taken by the profiler. A value of "start" causes the profiler thread to start collecting data if it is not already active. A value of "stop" causes the profiler thread to stop collecting data and write it to disk, and a value of "cancel" causes the profiler thread to stop collecting data and discard anything that has been captured. These operations occur immediately.

Default Value

none

Allowed Values

cancel

Stop collecting profile data and discard what has been captured.

none

Do not take any action.

start

Start collecting profile data.

stop

Stop collecting profile data and write what has been captured to a file in the profile directory.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-directory

Description

Specifies the path to the directory where profile information is to be written. This path may be either an absolute path or a path that is relative to the root of the OpenDJ directory server instance. The directory must exist and the directory server must have permission to create new files in it.

Default Value

None

Allowed Values

The path to any directory that exists on the filesystem and that can be read and written by the server user.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

profile-sample-interval

Description

Specifies the sample interval in milliseconds to be used when capturing profiling information in the server. When capturing data, the profiler thread sleeps for this length of time between calls to obtain traces for all threads running in the JVM.

Default Value

None

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.Upper limit is 2147483647 milliseconds.

Multi-valued

No

Required

Yes

Admin Action Required

None

Changes to this configuration attribute take effect the next time the profiler is started.

Advanced Property

No

Read-only

No

11 Referential Integrity Plugin

Plugins of type referential-integrity-plugin have the following properties:

attribute-type

Description

Specifies the attribute types for which referential integrity is to be maintained. At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34).

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN that limits the scope within which referential integrity is maintained.

Default Value

Referential integrity is maintained in all public naming contexts.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references

Description

Specifies whether reference attributes must refer to existing entries. When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-filter-criteria

Description

Specifies additional filter criteria which will be enforced when checking references. If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter.

Default Value

None

Allowed Values

An attribute-filter mapping.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

check-references-scope-criteria

Description

Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. The reference scope will only be enforced when reference checking is enabled.

Default Value

global

Allowed Values

global

References may refer to existing entries located anywhere in the Directory.

naming-context

References must refer to existing entries located within the same naming context.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.ReferentialIntegrityPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

log-file

Description

Specifies the log file location where the update records are written when the plug-in is in background-mode processing. The default location is the logs directory of the server instance, using the file name "referint".

Default Value

logs/referint

Allowed Values

A path to an existing file that is readable by the server.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

postoperationdelete

postoperationmodifydn

subordinatemodifydn

subordinatedelete

preoperationadd

preoperationmodify

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

update-interval

Description

Specifies the interval in seconds when referential integrity updates are made. If this value is 0, then the updates are made synchronously in the foreground.

Default Value

0 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Samba Password Plugin

Plugins of type samba-password-plugin have the following properties:

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SambaPasswordPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationmodify

postoperationextended

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

pwd-sync-policy

Description

Specifies which Samba passwords should be kept synchronized.

Default Value

sync-nt-password

Allowed Values

sync-lm-password

Synchronize the LanMan password attribute "sambaLMPassword"

sync-nt-password

Synchronize the NT password attribute "sambaNTPassword"

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

samba-administrator-dn

Description

Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped.

Default Value

Synchronize all updates to user passwords

Allowed Values

A valid DN.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Seven Bit Clean Plugin

Plugins of type seven-bit-clean-plugin have the following properties:

attribute-type

Description

Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean.

Default Value

uid

mail

userPassword

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN below which the checking is performed. Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed.

Default Value

All entries below all public naming contexts will be checked.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.SevenBitCleanPlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

ldifimport

preparseadd

preparsemodify

preparsemodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

14 Unique Attribute Plugin

Plugins of type unique-attribute-plugin have the following properties:

base-dn

Description

Specifies a base DN within which the attribute must be unique.

Default Value

The plug-in uses the server's public naming contexts in the searches.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the plug-in is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

invoke-for-internal-operations

Description

Indicates whether the plug-in should be invoked for internal operations. Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the plug-in implementation.

Default Value

org.opends.server.plugins.UniqueAttributePlugin

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.plugin.DirectoryServerPlugin

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

plugin-type

Description

Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked.

Default Value

preoperationadd

preoperationmodify

preoperationmodifydn

postoperationadd

postoperationmodify

postoperationmodifydn

postsynchronizationadd

postsynchronizationmodify

postsynchronizationmodifydn

Allowed Values

intermediateresponse

Invoked before sending an intermediate repsonse message to the client.

ldifexport

Invoked for each operation to be written during an LDIF export.

ldifimport

Invoked for each entry read during an LDIF import.

ldifimportbegin

Invoked at the beginning of an LDIF import session.

ldifimportend

Invoked at the end of an LDIF import session.

postconnect

Invoked whenever a new connection is established to the server.

postdisconnect

Invoked whenever an existing connection is terminated (by either the client or the server).

postoperationabandon

Invoked after completing the abandon processing.

postoperationadd

Invoked after completing the core add processing but before sending the response to the client.

postoperationbind

Invoked after completing the core bind processing but before sending the response to the client.

postoperationcompare

Invoked after completing the core compare processing but before sending the response to the client.

postoperationdelete

Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended

Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify

Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn

Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch

Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind

Invoked after completing the unbind processing.

postresponseadd

Invoked after sending the add response to the client.

postresponsebind

Invoked after sending the bind response to the client.

postresponsecompare

Invoked after sending the compare response to the client.

postresponsedelete

Invoked after sending the delete response to the client.

postresponseextended

Invoked after sending the extended response to the client.

postresponsemodify

Invoked after sending the modify response to the client.

postresponsemodifydn

Invoked after sending the modify DN response to the client.

postresponsesearch

Invoked after sending the search result done message to the client.

postsynchronizationadd

Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete

Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify

Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn

Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd

Invoked prior to performing the core add processing.

preoperationbind

Invoked prior to performing the core bind processing.

preoperationcompare

Invoked prior to performing the core compare processing.

preoperationdelete

Invoked prior to performing the core delete processing.

preoperationextended

Invoked prior to performing the core extended processing.

preoperationmodify

Invoked prior to performing the core modify processing.

preoperationmodifydn

Invoked prior to performing the core modify DN processing.

preoperationsearch

Invoked prior to performing the core search processing.

preparseabandon

Invoked prior to parsing an abandon request.

preparseadd

Invoked prior to parsing an add request.

preparsebind

Invoked prior to parsing a bind request.

preparsecompare

Invoked prior to parsing a compare request.

preparsedelete

Invoked prior to parsing a delete request.

preparseextended

Invoked prior to parsing an extended request.

preparsemodify

Invoked prior to parsing a modify request.

preparsemodifydn

Invoked prior to parsing a modify DN request.

preparsesearch

Invoked prior to parsing a search request.

preparseunbind

Invoked prior to parsing an unbind request.

searchresultentry

Invoked before sending a search result entry to the client.

searchresultreference

Invoked before sending a search result reference to the client.

shutdown

Invoked during a graceful directory server shutdown.

startup

Invoked during the directory server startup process.

subordinatedelete

Invoked in the course of deleting a subordinate entry of a delete operation.

subordinatemodifydn

Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation.

Multi-valued

Yes

Required

Yes

Admin Action Required

The Plugin must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

type

Description

Specifies the type of attributes to check for value uniqueness.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-plugin-root-prop

dsconfig set-plugin-root-prop — Modifies Plugin Root properties

dsconfig set-plugin-root-prop

```
dsconfig set-plugin-root-prop {options}
```

1 Description

Modifies Plugin Root properties.

2 Options

The **dsconfig set-plugin-root-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Plugin Root properties depend on the Plugin Root type, which depends on the null option.

3 Plugin Root

Plugin Roots of type plugin-root have the following properties:

plugin-order-intermediate-response

Description

Specifies the order in which intermediate response plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which intermediate response plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-export

Description

Specifies the order in which LDIF export plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the

plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF export plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import

Description

Specifies the order in which LDIF import plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-begin

Description

Specifies the order in which LDIF import begin plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import begin plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-ldif-import-end

Description

Specifies the order in which LDIF import end plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which LDIF import end plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-connect

Description

Specifies the order in which post-connect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-connect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-disconnect

Description

Specifies the order in which post-disconnect plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-disconnect plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-abandon

Description

Specifies the order in which post-operation abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-add

Description

Specifies the order in which post-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-bind

Description

Specifies the order in which post-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-compare

Description

Specifies the order in which post-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-

in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-delete

Description

Specifies the order in which post-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-extended

Description

Specifies the order in which post-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify

Description

Specifies the order in which post-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-modify-dn

Description

Specifies the order in which post-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-search

Description

Specifies the order in which post-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-operation-unbind

Description

Specifies the order in which post-operation unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-operation unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-add

Description

Specifies the order in which post-response add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-bind

Description

Specifies the order in which post-response bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-compare

Description

Specifies the order in which post-response compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-

in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-delete

Description

Specifies the order in which post-response delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-extended

Description

Specifies the order in which post-response extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify

Description

Specifies the order in which post-response modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-modify-dn

Description

Specifies the order in which post-response modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-response-search

Description

Specifies the order in which post-response search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-response search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-add

Description

Specifies the order in which post-synchronization add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-delete

Description

Specifies the order in which post-synchronization delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify

Description

Specifies the order in which post-synchronization modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-post-synchronization-modify-dn

Description

Specifies the order in which post-synchronization modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of

plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which post-synchronization modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-add

Description

Specifies the order in which pre-operation add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-bind

Description

Specifies the order in which pre-operation bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-compare

Description

Specifies the order in which pre-operation compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-delete

Description

Specifies the order in which pre-operation delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-extended

Description

Specifies the order in which pre-operation extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify

Description

Specifies the order in which pre-operation modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-modify-dn

Description

Specifies the order in which pre-operation modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-operation-search

Description

Specifies the order in which pre-operation search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-operation searc plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-abandon

Description

Specifies the order in which pre-parse abandon plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where

the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse abandon plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-add

Description

Specifies the order in which pre-parse add plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse add plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-bind

Description

Specifies the order in which pre-parse bind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse bind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-compare

Description

Specifies the order in which pre-parse compare plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse compare plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-delete

Description

Specifies the order in which pre-parse delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-extended

Description

Specifies the order in which pre-parse extended operation plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse extended operation plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify

Description

Specifies the order in which pre-parse modify plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-modify-dn

Description

Specifies the order in which pre-parse modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-search

Description

Specifies the order in which pre-parse search plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse search plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-pre-parse-unbind

Description

Specifies the order in which pre-parse unbind plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where

the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which pre-parse unbind plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-entry

Description

Specifies the order in which search result entry plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result entry plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-search-result-reference

Description

Specifies the order in which search result reference plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which search result reference plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-shutdown

Description

Specifies the order in which shutdown plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which shutdown plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-startup

Description

Specifies the order in which startup plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which startup plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-delete

Description

Specifies the order in which subordinate delete plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate delete plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

plugin-order-subordinate-modify-dn

Description

Specifies the order in which subordinate modify DN plug-ins are to be loaded and invoked. The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined).

Default Value

The order in which subordinate modify DN plug-ins are loaded and invoked is undefined.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-replication-domain-prop

dsconfig set-replication-domain-prop — Modifies Replication Domain properties

dsconfig set-replication-domain-prop

`dsconfig set-replication-domain-prop` {options}

1 Description

Modifies Replication Domain properties.

2 Options

The **dsconfig set-replication-domain-prop** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--domain-name {name}`

The name of the Replication Domain.

Replication Domain properties depend on the Replication Domain type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Domain types:

replication-domain

Default {name}: Replication Domain

Enabled by default: false

See the section called “Replication Domain” for the properties of this Replication Domain type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Replication Domain properties depend on the Replication Domain type, which depends on the `--domain-name {name}` option.

3 Replication Domain

Replication Domains of type replication-domain have the following properties:

assured-sd-level

Description

The level of acknowledgment for Safe Data assured sub mode. When assured replication is configured in Safe Data mode, this value defines

the number of replication servers (with the same group ID of the local server) that should acknowledge the sent update before the LDAP client call can return.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-timeout

Description

The timeout value when waiting for assured replication acknowledgments. Defines the amount of milliseconds the server will wait for assured acknowledgments (in either Safe Data or Safe Read assured replication modes) before returning anyway the LDAP client call.

Default Value

2000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second,

and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

assured-type

Description

Defines the assured replication mode of the replicated domain. The assured replication can be disabled or enabled. When enabled, two modes are available: Safe Data or Safe Read modes.

Default Value

not-assured

Allowed Values

not-assured

Assured replication is not enabled. Updates sent for replication (for being replayed on other LDAP servers in the topology) are sent without waiting for any acknowledgment and the LDAP client call returns immediately.

safe-data

Assured replication is enabled in Safe Data mode: updates sent for replication are subject to acknowledgment from the replication servers that have the same group ID as the local server (defined with the group-id property). The number of acknowledgments to expect is defined by the assured-sd-level property. After acknowledgments are received, LDAP client call returns.

safe-read

Assured replication is enabled in Safe Read mode: updates sent for replication are subject to acknowledgments from the LDAP servers in the topology that have the same group ID as the local server (defined with the group-id property). After acknowledgments are received, LDAP client call returns.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DN of the replicated data.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

changetime-heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when sending its local change time to the Replication Server. The directory server sends a regular heart-beat to the Replication within the specified interval. The heart-beat indicates the change time of the directory server to the Replication Server.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in

milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

conflicts-historical-purge-delay

Description

This delay indicates the time (in minutes) the domain keeps the historical information necessary to solve conflicts.When a change stored in the historical part of the user entry has a date (from its replication ChangeNumber) older than this delay, it is candidate to be purged. The purge is applied on 2 events: modify of the entry, dedicated purge task.

Default Value

1440m

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 minutes.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-exclude

Description

Allows to exclude some attributes to replicate to this server. If fractional-exclude configuration attribute is used, attributes specified in this

attribute will be ignored (not added/modified/deleted) when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

fractional-include

Description

Allows to include some attributes to replicate to this server. If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute.

Default Value

None

Allowed Values

The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group ID associated with this replicated domain. This value defines the group ID of the replicated domain. The replication system will preferably connect and send updates to replicate to a replication server with the same group ID as its own one (the local server group ID).

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

heartbeat-interval

Description

Specifies the heart-beat interval that the directory server will use when communicating with Replication Servers. The directory server expects a regular heart-beat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server.

Default Value

10000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 100 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

initialization-window-size

Description

Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization.

Default Value

100

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

isolation-policy

Description

Specifies the behavior of the directory server if a write operation is attempted on the data within the Replication Domain when none of the configured Replication Servers are available.

Default Value

reject-all-updates

Allowed Values

accept-all-updates

Indicates that updates should be accepted even though it is not possible to send them to any Replication Server. Best effort is made to re-send those updates to a Replication Servers when one of them is available, however those changes are at risk because they are only available from the historical information. This mode can also introduce high replication latency.

reject-all-updates

Indicates that all updates attempted on this Replication Domain are rejected when no Replication Server is available.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

log-changenumber

Description

Indicates if this server logs the ChangeNumber in access log. This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

referrals-url

Description

The URLs other LDAP servers should use to refer to the local server. URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used.

Default Value

None

Allowed Values

A LDAP URL compliant with RFC 2255.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of the Replication Servers within the Replication Domain to which the directory server should try to connect at startup time. Addresses must be specified using the syntax: hostname:port

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

server-id

Description

Specifies a unique identifier for the directory server within the Replication Domain. Each directory server within the same Replication Domain must have a different server ID. A directory server which is a member of multiple Replication Domains may use the same server ID for each of its Replication Domain configurations.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

solve-conflicts

Description

Indicates if this server solves conflict. This boolean indicates if this domain keeps the historical information necessary to solve conflicts.

When set to false the server will not maintain historical information and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the directory server will use when communicating with Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-replication-server-prop

dsconfig set-replication-server-prop — Modifies Replication Server properties

dsconfig set-replication-server-prop

`dsconfig set-replication-server-prop {options}`

1 Description

Modifies Replication Server properties.

2 Options

The **dsconfig set-replication-server-prop** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Replication Server properties depend on the Replication Server type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Replication Server types:

replication-server

Default {name}: Replication Server

Enabled by default: false

See the section called “Replication Server” for the properties of this Replication Server type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Replication Server properties depend on the Replication Server type, which depends on the `--provider-name {name}` option.

3 Replication Server

Replication Servers of type replication-server have the following properties:

assured-timeout

Description

The timeout value when waiting for assured mode acknowledgments. Defines the number of milliseconds that the replication server will wait for assured acknowledgments (in either Safe Data or Safe Read assured sub modes) before forgetting them and answer to the entity that sent an update and is waiting for acknowledgment.

Default Value

1000ms

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds

- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

cipher-key-length

Description

Specifies the key length in bits for the preferred cipher.

Default Value

128

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

cipher-transformation

Description

Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding.

Default Value

AES/CBC/PKCS5Padding

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect cryptographic operations performed after the change.

Advanced Property

No

Read-only

No

compute-change-number

Description

Whether the replication server will compute change numbers. This boolean tells the replication server to compute change numbers for each replicated change by maintaining a change number index database. Changenumbers are computed according to http://tools.ietf.org/html/draft-good-ldap-changelog-04. Note this functionality has an impact on CPU, disk accesses and storage. If changenumbers are not required, it is advisable to set this value to false.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

confidentiality-enabled

Description

Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately but only affect operations performed after the change.

Advanced Property

No

Read-only

No

degraded-status-threshold

Description

The number of pending changes as threshold value for putting a directory server in degraded status. This value represents a number of pending

changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status.

Default Value

5000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-id

Description

The group id for the replication server. This value defines the group id of the replication server. The replication system of a LDAP server uses the group id of the replicated domain and tries to connect, if possible, to a replication with the same group id.

Default Value

1

Allowed Values

An integer value. Lower value is 1. Upper value is 127.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

monitoring-period

Description

The period between sending of monitoring messages. Defines the duration that the replication server will wait before sending new monitoring messages to its peers (replication servers and directory servers). Larger values increase the length of time it takes for a directory server to detect and switch to a more suitable replication server, whereas smaller values increase the amount of background network traffic.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

queue-size

Description

Specifies the number of changes that are kept in memory for each directory server in the Replication Domain.

Default Value

10000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

replication-db-directory

Description

The path where the Replication Server stores all persistent information.

Default Value

changelogDb

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

replication-port

Description

The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-purge-delay

Description

The time (in seconds) after which the Replication Server erases all persistent information.

Default Value

3 days

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds

- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the addresses of other Replication Servers to which this Replication Server tries to connect at startup time. Addresses must be specified using the syntax: "hostname:port". If IPv6 addresses are used as the hostname, they must be specified using the syntax "[IPv6Address]:port".

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server-id

Description

Specifies a unique identifier for the Replication Server. Each Replication Server must have a different server ID.

Default Value

None

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

Yes

source-address

Description

If specified, the server will bind to the address before connecting to the remote server. The address must be one assigned to an existing network interface.

Default Value

Let the server decide.

Allowed Values

An IP address

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

weight

Description

The weight of the replication server. The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different

power and one wants to spread the load between the replication servers according to their power.

Default Value

1

Allowed Values

An integer value. Lower value is 1.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

window-size

Description

Specifies the window size that the Replication Server uses when communicating with other Replication Servers. This option may be deprecated and removed in future releases.

Default Value

100000

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-root-dn-prop

dsconfig set-root-dn-prop — Modifies Root DN properties

dsconfig set-root-dn-prop

```
dsconfig set-root-dn-prop {options}
```

1 Description

Modifies Root DN properties.

2 Options

The **dsconfig set-root-dn-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Root DN properties depend on the Root DN type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Root DN properties depend on the Root DN type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Root DN properties depend on the Root DN type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Root DN properties depend on the Root DN type, which depends on the null option.

3 Root DN

Root Dns of type root-dn have the following properties:

default-root-privilege-name

Description

Specifies the names of the privileges that root users will be granted by default.

Default Value

bypass-lockdown

bypass-acl

modify-acl

config-read

config-write

ldif-import

ldif-export

backend-backup

backend-restore

server-lockdown

server-shutdown

server-restart

disconnect-client

cancel-request

password-reset

update-schema

privilege-change

unindexed-search

subentry-write

changelog-read

Allowed Values

backend-backup

Allows the user to request that the server process backup tasks.

backend-restore

Allows the user to request that the server process restore tasks.

bypass-acl

Allows the associated user to bypass access control checks performed by the server.

bypass-lockdown

Allows the associated user to bypass server lockdown mode.

cancel-request

Allows the user to cancel operations in progress on other client connections.

changelog-read

Allows the user to perform read operations on the changelog

config-read

Allows the associated user to read the server configuration.

config-write

Allows the associated user to update the server configuration. The config-read privilege is also required.

data-sync

Allows the user to participate in data synchronization.

disconnect-client

Allows the user to terminate other client connections.

jmx-notify

Allows the associated user to subscribe to receive JMX notifications.

jmx-read

Allows the associated user to perform JMX read operations.

jmx-write

Allows the associated user to perform JMX write operations.

ldif-export

Allows the user to request that the server process LDIF export tasks.

ldif-import

Allows the user to request that the server process LDIF import tasks.

modify-acl

Allows the associated user to modify the server's access control configuration.

password-reset

Allows the user to reset user passwords.

privilege-change

Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users.

proxied-auth

Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.

server-lockdown

Allows the user to place and bring the server of lockdown mode.

server-restart

Allows the user to request that the server perform an in-core restart.

server-shutdown

Allows the user to request that the server shut down.

subentry-write

Allows the associated user to perform LDAP subentry write operations.

unindexed-search

Allows the user to request that the server process a search that cannot be optimized using server indexes.

update-schema

Allows the user to make changes to the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-root-dse-backend-prop

dsconfig set-root-dse-backend-prop — Modifies Root DSE Backend properties

dsconfig set-root-dse-backend-prop

```
dsconfig set-root-dse-backend-prop {options}
```

1 Description

Modifies Root DSE Backend properties.

2 Options

The **dsconfig set-root-dse-backend-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Root DSE Backend properties depend on the Root DSE Backend type, which depends on the null option.

3 Root DSE Backend

Root DSE Backends of type root-dse-backend have the following properties:

show-all-attributes

Description

Indicates whether all attributes in the root DSE are to be treated like user attributes (and therefore returned to clients by default) regardless of the directory server schema configuration.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

show-subordinate-naming-contexts

Description

Indicates whether subordinate naming contexts should be visible in the namingContexts attribute of the RootDSE. By default only top level naming contexts are visible

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-sasl-mechanism-handler-prop

dsconfig set-sasl-mechanism-handler-prop — Modifies SASL Mechanism Handler properties

dsconfig set-sasl-mechanism-handler-prop

`dsconfig set-sasl-mechanism-handler-prop {options}`

1 Description

Modifies SASL Mechanism Handler properties.

2 Options

The **dsconfig set-sasl-mechanism-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following SASL Mechanism Handler types:

anonymous-sasl-mechanism-handler

Default {name}: Anonymous SASL Mechanism Handler

Enabled by default: true

See the section called “Anonymous SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

cram-md5-sasl-mechanism-handler

Default {name}: Cram MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Cram MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

digest-md5-sasl-mechanism-handler

Default {name}: Digest MD5 SASL Mechanism Handler

Enabled by default: true

See the section called “Digest MD5 SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

external-sasl-mechanism-handler

Default {name}: External SASL Mechanism Handler

Enabled by default: true

See the section called “External SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

gssapi-sasl-mechanism-handler

Default {name}: GSSAPI SASL Mechanism Handler

Enabled by default: true

See the section called “GSSAPI SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

plain-sasl-mechanism-handler

Default {name}: Plain SASL Mechanism Handler

Enabled by default: true

See the section called “Plain SASL Mechanism Handler” for the properties of this SASL Mechanism Handler type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

SASL Mechanism Handler properties depend on the SASL Mechanism Handler type, which depends on the `--handler-name {name}` option.

3 Anonymous SASL Mechanism Handler

SASL Mechanism Handlers of type anonymous-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.AnonymousSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Cram MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type cram-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Cram MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.CRAMMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

5 Digest MD5 SASL Mechanism Handler

SASL Mechanism Handlers of type digest-md5-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Digest MD5 SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.DigestMD5SASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Default Value

If this value is not provided, then the server defaults to use the fully qualified hostname of the machine.

Allowed Values

Any realm string that does not contain a comma.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. If this configuration attribute is present, then

the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value.

Default Value

The server attempts to determine the fully-qualified domain name dynamically.

Allowed Values

The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 External SASL Mechanism Handler

SASL Mechanism Handlers of type external-sasl-mechanism-handler have the following properties:

certificate-attribute

Description

Specifies the name of the attribute to hold user certificates. This property must specify the name of a valid attribute type defined in the server schema.

Default Value

userCertificate

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-mapper

Description

Specifies the name of the certificate mapper that should be used to match client certificates to user entries.

Default Value

None

Allowed Values

The DN of any Certificate Mapper. The referenced certificate mapper must be enabled when the External SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

certificate-validation-policy

Description

Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry.

Default Value

None

Allowed Values

always

Always require the peer certificate to be present in the user's entry.

ifpresent

If the user's entry contains one or more certificates, require that one of them match the peer certificate.

never

Do not look for the peer certificate to be present in the user's entry.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.ExternalSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

7 GSSAPI SASL Mechanism Handler

SASL Mechanism Handlers of type gssapi-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the GSSAPI SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.GSSAPISASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

kdc-address

Description

Specifies the address of the KDC that is to be used for Kerberos processing. If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration.

Default Value

The server attempts to determine the KDC address from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

keytab

Description

Specifies the path to the keytab file that should be used for Kerberos processing. If provided, this is either an absolute path or one that is relative to the server instance root.

Default Value

The server attempts to use the system-wide default keytab.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

principal-name

Description

Specifies the principal name. It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/".

Default Value

The server attempts to determine the principal name from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

quality-of-protection

Description

The name of a property that specifies the quality of protection the server will support.

Default Value

none

Allowed Values

confidentiality

Quality of protection equals authentication with integrity and confidentiality protection.

integrity

Quality of protection equals authentication with integrity protection.

none

QOP equals authentication only.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

realm

Description

Specifies the realm to be used for GSSAPI authentication.

Default Value

The server attempts to determine the realm from the underlying system configuration.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

server-fqdn

Description

Specifies the DNS-resolvable fully-qualified domain name for the system.

Default Value

The server attempts to determine the fully-qualified domain name dynamically .

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Plain SASL Mechanism Handler

SASL Mechanism Handlers of type plain-sasl-mechanism-handler have the following properties:

enabled

Description

Indicates whether the SASL mechanism handler is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

identity-mapper

Description

Specifies the name of the identity mapper that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory.

Default Value

None

Allowed Values

The DN of any Identity Mapper. The referenced identity mapper must be enabled when the Plain SASL Mechanism Handler is enabled.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation.

Default Value

org.opends.server.extensions.PlainSASLMechanismHandler

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SASLMechanismHandler

Multi-valued

No

Required

Yes

Admin Action Required

The SASL Mechanism Handler must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-schema-provider-prop

dsconfig set-schema-provider-prop — Modifies Schema Provider properties

dsconfig set-schema-provider-prop

```
dsconfig set-schema-provider-prop {options}
```

1 Description

Modifies Schema Provider properties.

2 Options

The **dsconfig set-schema-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Schema Provider.

Schema Provider properties depend on the Schema Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Schema Provider types:

core-schema

Default {name}: Core Schema

Enabled by default: true

See the section called “Core Schema” for the properties of this Schema Provider type.

json-schema

Default {name}: Json Schema

Enabled by default: true

See the section called “Json Schema” for the properties of this Schema Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Schema Provider properties depend on the Schema Provider type, which depends on the `--provider-name {name}` option.

3 Core Schema

Schema Providers of type core-schema have the following properties:

allow-attribute-types-with-no-sup-or-syntax

Description

Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax When set to true, invalid attribute type definitions will use the default syntax.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

allow-zero-length-values-directory-string

Description

Indicates whether zero-length (that is, an empty string) values are allowed for directory string. This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

disabled-matching-rule

Description

The set of disabled matching rules. Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled matching rule.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

disabled-syntax

Description

The set of disabled syntaxes. Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value.

Default Value

NONE

Allowed Values

The OID of the disabled syntax, or NONE

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Core Schema implementation.

Default Value

org.opends.server.schema.CoreSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

json-validation-policy

Description

Specifies the policy that will be used when validating JSON syntax values.

Default Value

strict

Allowed Values

disabled

JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.

lenient

JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.

strict

JSON syntax values must strictly conform to RFC 7159.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-certificates

Description

Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-country-string

Description

Indicates whether country code values are required to strictly comply with the standard definition for this syntax. When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-jpeg-photos

Description

Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strict-format-telephone-numbers

Description

Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

strip-syntax-min-upper-bound-attribute-type-description

Description

Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option allows the server to be configured to provide schema definitions these APIs can parse correctly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 Json Schema

Schema Providers of type json-schema have the following properties:

case-sensitive-strings

Description

Indicates whether JSON string comparisons should be case-sensitive.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Schema Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ignore-white-space

Description

Indicates whether JSON string comparisons should ignore white-space. When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character.

Default Value

true

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

indexed-field

Description

Specifies which JSON fields should be indexed. A field will be indexed if it matches any of the configured field patterns.

Default Value

All JSON fields will be indexed.

Allowed Values

A JSON pointer which may include wild-cards. A single '*' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Json Schema implementation.

Default Value

org.opends.server.schema.JsonSchemaProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.schema.SchemaProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

matching-rule-name

Description

The name of the custom JSON matching rule.

Default Value

The matching rule will not have a name.

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

matching-rule-oid

Description

The numeric OID of the custom JSON matching rule.

Default Value

None

Allowed Values

The OID of the matching rule.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-service-discovery-mechanism-prop

dsconfig set-service-discovery-mechanism-prop — Modifies Service Discovery Mechanism properties

dsconfig set-service-discovery-mechanism-prop

```
dsconfig set-service-discovery-mechanism-prop {options}
```

1 Description

Modifies Service Discovery Mechanism properties.

2 Options

The **dsconfig set-service-discovery-mechanism-prop** command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Service Discovery Mechanism types:

replication-service-discovery-mechanism

Default {name}: Replication Service Discovery Mechanism

Enabled by default: false

See the section called “Replication Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

static-service-discovery-mechanism

Default {name}: Static Service Discovery Mechanism

Enabled by default: false

See the section called “Static Service Discovery Mechanism” for the properties of this Service Discovery Mechanism type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Service Discovery Mechanism properties depend on the Service Discovery Mechanism type, which depends on the `--mechanism-name {name}` option.

3 Replication Service Discovery Mechanism

Service Discovery Mechanisms of type replication-service-discovery-mechanism have the following properties:

bind-dn

Description

The bind DN for periodically reading replication server configurations The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

bind-password

Description

The bind password for periodically reading replication server configurations The bind password must be the same on all replication and directory servers

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

discovery-interval

Description

Interval between two replication server configuration discovery queries. Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.ReplicationServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-group-id

Description

Replication domain group ID of preferred directory server replicas. Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable.

Default Value

All the server replicas will be treated the same.

Allowed Values

An integer value. Lower value is 0.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

replication-server

Description

Specifies the list of replication servers to contact periodically when discovering server replicas.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

4 Static Service Discovery Mechanism

Service Discovery Mechanisms of type static-service-discovery-mechanism have the following properties:

discovery-interval

Description

Interval between two server configuration discovery executions. Specifies how frequently to read the configuration of the servers in order to discover their new information.

Default Value

60s

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes

- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 1 seconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation.

Default Value

org.opends.server.backends.proxy.StaticServiceDiscoveryMechanism

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.backends.proxy.ServiceDiscoveryMechanism

Multi-valued

No

Required

Yes

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

key-manager-provider

Description

Specifies the name of the key manager that should be used with this Service Discovery Mechanism.

Default Value

None

Allowed Values

The DN of any Key Manager Provider. The referenced key manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections.

Advanced Property

No

Read-only

No

primary-server

Description

Specifies a list of servers that will be used in preference to secondary servers when available.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

secondary-server

Description

Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable.

Default Value

None

Allowed Values

A host name followed by a ":" and a port number.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

ssl-cert-nickname

Description

Specifies the nicknames (also called the aliases) of the keys or key pairs that the Service Discovery Mechanism should use when performing SSL communication. The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Service Discovery Mechanism is configured to use SSL.

Default Value

Let the server decide.

Allowed Values

A String

Multi-valued

Yes

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

trust-manager-provider

Description

Specifies the name of the trust manager that should be used with the Service Discovery Mechanism.

Default Value

Use the trust manager provided by the JVM.

Allowed Values

The DN of any Trust Manager Provider. The referenced trust manager provider must be enabled when the Service Discovery Mechanism is enabled and configured to use SSL or StartTLS.

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections.

Advanced Property

No

Read-only

No

use-ssl

Description

Indicates whether the Service Discovery Mechanism should use SSL. If enabled, the Service Discovery Mechanism will use SSL to encrypt communication with the clients.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

use-start-tls

Description

Indicates whether the Service Discovery Mechanism should use Start TLS. If enabled, the Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

No

Admin Action Required

The Service Discovery Mechanism must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

No

Read-only

No

dsconfig set-synchronization-provider-prop

dsconfig set-synchronization-provider-prop — Modifies Synchronization Provider properties

dsconfig set-synchronization-provider-prop

```
dsconfig set-synchronization-provider-prop {options}
```

1 Description

Modifies Synchronization Provider properties.

2 Options

The **dsconfig set-synchronization-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Synchronization Provider.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Synchronization Provider types:

replication-synchronization-provider

Default {name}: Replication Synchronization Provider

Enabled by default: true

See the section called “Replication Synchronization Provider” for the properties of this Synchronization Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Synchronization Provider properties depend on the Synchronization Provider type, which depends on the `--provider-name {name}` option.

3 Replication Synchronization Provider

Synchronization Providers of type replication-synchronization-provider have the following properties:

connection-timeout

Description

Specifies the timeout used when connecting to peers and when performing SSL negotiation.

Default Value

5 seconds

Allowed Values

Some property values take a time duration. Durations are expressed as numbers followed by units. For example `1 s` means one second, and `2 w` means two weeks. Some durations have minimum granularity or maximum units, so you cannot necessary specify every duration in milliseconds or weeks for example. Some durations allow you to use a special value to mean unlimited. Units are specified as follows.

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks

Lower limit is 0 milliseconds.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Synchronization Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation.

Default Value

org.opends.server.replication.plugin.MultimasterReplication

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.SynchronizationProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-update-replay-threads

Description

Specifies the number of update replay threads. This value is the number of threads created for replaying every updates received for all the replication domains.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 65535.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

dsconfig set-trust-manager-provider-prop

dsconfig set-trust-manager-provider-prop — Modifies Trust Manager Provider properties

dsconfig set-trust-manager-provider-prop

```
dsconfig set-trust-manager-provider-prop {options}
```

1 Description

Modifies Trust Manager Provider properties.

2 Options

The **dsconfig set-trust-manager-provider-prop** command takes the following options:

`--provider-name {name}`

The name of the Trust Manager Provider.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Trust Manager Provider types:

blind-trust-manager-provider

Default {name}: Blind Trust Manager Provider

Enabled by default: true

See the section called “Blind Trust Manager Provider” for the properties of this Trust Manager Provider type.

file-based-trust-manager-provider

Default {name}: File Based Trust Manager Provider

Enabled by default: true

See the section called “File Based Trust Manager Provider” for the properties of this Trust Manager Provider type.

ldap-trust-manager-provider

Default {name}: LDAP Trust Manager Provider

Enabled by default: true

See the section called “LDAP Trust Manager Provider” for the properties of this Trust Manager Provider type.

pkcs11-trust-manager-provider

Default {name}: PKCS11 Trust Manager Provider

Enabled by default: true

See the section called “PKCS11 Trust Manager Provider” for the properties of this Trust Manager Provider type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Trust Manager Provider properties depend on the Trust Manager Provider type, which depends on the `--provider-name {name}` option.

3 Blind Trust Manager Provider

Trust Manager Providers of type blind-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.BlindTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

4 File Based Trust Manager Provider

Trust Manager Providers of type file-based-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.FileBasedTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-file

Description

Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root.

Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

An absolute path or a path that is relative to the OpenDJ directory server instance root.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the File Based Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-type

Description

Specifies the format for the data in the trust store file. Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed.

Default Value

None

Allowed Values

Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 LDAP Trust Manager Provider

Trust Manager Providers of type ldap-trust-manager-provider have the following properties:

base-dn

Description

The base DN beneath which LDAP key store entries are located.

Default Value

None

Allowed Values

A valid DN.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.LDAPTrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the LDAP Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

6 PKCS11 Trust Manager Provider

Trust Manager Providers of type pkcs11-trust-manager-provider have the following properties:

enabled

Description

Indicate whether the Trust Manager Provider is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

The fully-qualified name of the Java class that provides the PKCS11 Trust Manager Provider implementation.

Default Value

org.opends.server.extensions.PKCS11TrustManagerProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.TrustManagerProvider

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

trust-store-pin

Description

Specifies the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-environment-variable

Description

Specifies the name of the environment variable that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-file

Description

Specifies the path to the text file whose only contents should be a single line containing the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

trust-store-pin-property

Description

Specifies the name of the Java property that contains the clear-text PIN needed to access the PKCS11 Trust Manager Provider .

Default Value

None

Allowed Values

A String

Multi-valued

No

Required

No

Admin Action Required

None

Changes to this property will take effect the next time that the PKCS11 Trust Manager Provider is accessed.

Advanced Property

No

Read-only

No

dsconfig set-virtual-attribute-prop

dsconfig set-virtual-attribute-prop — Modifies Virtual Attribute properties

dsconfig set-virtual-attribute-prop

```
dsconfig set-virtual-attribute-prop {options}
```

1 Description

Modifies Virtual Attribute properties.

2 Options

The **dsconfig set-virtual-attribute-prop** command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the {name} you provide.

By default, OpenDJ directory server supports the following Virtual Attribute types:

collective-attribute-subentries-virtual-attribute

Default {name}: Collective Attribute Subentries Virtual Attribute

Enabled by default: true

See the section called “Collective Attribute Subentries Virtual Attribute” for the properties of this Virtual Attribute type.

entity-tag-virtual-attribute

Default {name}: Entity Tag Virtual Attribute

Enabled by default: true

See the section called “Entity Tag Virtual Attribute” for the properties of this Virtual Attribute type.

entry-dn-virtual-attribute

Default {name}: Entry DN Virtual Attribute

Enabled by default: true

See the section called “Entry DN Virtual Attribute” for the properties of this Virtual Attribute type.

entry-uuid-virtual-attribute

Default {name}: Entry UUID Virtual Attribute

Enabled by default: true

See the section called “Entry UUID Virtual Attribute” for the properties of this Virtual Attribute type.

governing-structure-rule-virtual-attribute

Default {name}: Governing Structure Rule Virtual Attribute

Enabled by default: true

See the section called “Governing Structure Rule Virtual Attribute” for the properties of this Virtual Attribute type.

has-subordinates-virtual-attribute

Default {name}: Has Subordinates Virtual Attribute

Enabled by default: true

See the section called “Has Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

is-member-of-virtual-attribute

Default {name}: Is Member Of Virtual Attribute

Enabled by default: true

See the section called “Is Member Of Virtual Attribute” for the properties of this Virtual Attribute type.

member-virtual-attribute

Default {name}: Member Virtual Attribute

Enabled by default: true

See the section called “Member Virtual Attribute” for the properties of this Virtual Attribute type.

num-subordinates-virtual-attribute

Default {name}: Num Subordinates Virtual Attribute

Enabled by default: true

See the section called “Num Subordinates Virtual Attribute” for the properties of this Virtual Attribute type.

password-expiration-time-virtual-attribute

Default {name}: Password Expiration Time Virtual Attribute

Enabled by default: true

See the section called “Password Expiration Time Virtual Attribute” for the properties of this Virtual Attribute type.

password-policy-subentry-virtual-attribute

Default {name}: Password Policy Subentry Virtual Attribute

Enabled by default: true

See the section called “Password Policy Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

structural-object-class-virtual-attribute

Default {name}: Structural Object Class Virtual Attribute

Enabled by default: true

See the section called “Structural Object Class Virtual Attribute” for the properties of this Virtual Attribute type.

subschema-subentry-virtual-attribute

Default {name}: Subschema Subentry Virtual Attribute

Enabled by default: true

See the section called “Subschema Subentry Virtual Attribute” for the properties of this Virtual Attribute type.

user-defined-virtual-attribute

Default {name}: User Defined Virtual Attribute

Enabled by default: true

See the section called “User Defined Virtual Attribute” for the properties of this Virtual Attribute type.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Virtual Attribute properties depend on the Virtual Attribute type, which depends on the `--name {name}` option.

3 Collective Attribute Subentries Virtual Attribute

Virtual Attributes of type collective-attribute-subentries-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

collectiveAttributeSubentries

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Entity Tag Virtual Attribute

Virtual Attributes of type entity-tag-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

etag

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

checksum-algorithm

Description

The algorithm which should be used for calculating the entity tag checksum value.

Default Value

adler-32

Allowed Values

adler-32

The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.

crc-32

The CRC-32 checksum algorithm.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

excluded-attribute

Description

The list of attributes which should be ignored when calculating the entity tag checksum value. Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum.

Default Value

ds-sync-hist

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntityTagVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

5 Entry DN Virtual Attribute

Virtual Attributes of type entry-dn-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryDN

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryDNVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

6 Entry UUID Virtual Attribute

Virtual Attributes of type entry-uuid-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

entryUUID

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.EntryUUIDVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

7 Governing Structure Rule Virtual Attribute

Virtual Attributes of type governing-structure-rule-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

governingStructureRule

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

8 Has Subordinates Virtual Attribute

Virtual Attributes of type has-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

hasSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

9 Is Member Of Virtual Attribute

Virtual Attributes of type is-member-of-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

isMemberOf

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.IsMemberOfVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

10 Member Virtual Attribute

Virtual Attributes of type member-virtual-attribute have the following properties:

allow-retrieving-membership

Description

Indicates whether to handle requests that request all values for the virtual attribute. This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly.

Default Value

false

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or

more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.MemberVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

11 Num Subordinates Virtual Attribute

Virtual Attributes of type num-subordinates-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

numSubordinates

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

12 Password Expiration Time Virtual Attribute

Virtual Attributes of type password-expiration-time-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

ds-pwp-password-expiration-time

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

13 Password Policy Subentry Virtual Attribute

Virtual Attributes of type password-policy-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

pwdPolicySubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

14 Structural Object Class Virtual Attribute

Virtual Attributes of type structural-object-class-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

structuralObjectClass

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values

are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

15 Subschema Subentry Virtual Attribute

Virtual Attributes of type subschema-subentry-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

subschemaSubentry

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

virtual-overrides-real

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

16 User Defined Virtual Attribute

Virtual Attributes of type user-defined-virtual-attribute have the following properties:

attribute-type

Description

Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute.

Default Value

None

Allowed Values

The name of an attribute type defined in the server schema.

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

base-dn

Description

Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. If no values are given, then the server generates virtual attributes anywhere in the server.

Default Value

The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

conflict-behavior

Description

Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute.

Default Value

real-overrides-virtual

Allowed Values

merge-real-and-virtual

Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.

real-overrides-virtual

Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.

virtual-overrides-real

Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

enabled

Description

Indicates whether the Virtual Attribute is enabled for use.

Default Value

None

Allowed Values

true

false

Multi-valued

No

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

filter

Description

Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute.

Default Value

(objectClass=*)

Allowed Values

Any valid search filter string.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

group-dn

Description

Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute.

Default Value

Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute.

Allowed Values

A valid DN.

Multi-valued

Yes

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

java-class

Description

Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values.

Default Value

org.opends.server.extensions.UserDefinedVirtualAttributeProvider

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.VirtualAttributeProvider

Multi-valued

No

Required

Yes

Admin Action Required

The Virtual Attribute must be disabled and re-enabled for changes to this setting to take effect

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

scope

Description

Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute.

Default Value

whole-subtree

Allowed Values

base-object

Search the base object only.

single-level

Search the immediate children of the base object but do not include any of their descendants or the base object itself.

subordinate-subtree

Search the entire subtree below the base object but do not include the base object itself.

whole-subtree

Search the base object and the entire subtree below the base object.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

value

Description

Specifies the values to be included in the virtual attribute.

Default Value

None

Allowed Values

A String

Multi-valued

Yes

Required

Yes

Admin Action Required

None

Advanced Property

No

Read-only

No

dsconfig set-work-queue-prop

dsconfig set-work-queue-prop — Modifies Work Queue properties

dsconfig set-work-queue-prop

```
dsconfig set-work-queue-prop {options}
```

1 Description

Modifies Work Queue properties.

2 Options

The **dsconfig set-work-queue-prop** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Work Queue properties depend on the Work Queue type, which depends on the null option.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

Work Queue properties depend on the Work Queue type, which depends on the null option.

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

Work Queue properties depend on the Work Queue type, which depends on the null option.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

Work Queue properties depend on the Work Queue type, which depends on the null option.

3 Parallel Work Queue

Work Queues of type parallel-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Parallel Work Queue implementation.

Default Value

org.opends.server.extensions.ParallelWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

4 Traditional Work Queue

Work Queues of type traditional-work-queue have the following properties:

java-class

Description

Specifies the fully-qualified name of the Java class that provides the Traditional Work Queue implementation.

Default Value

org.opends.server.extensions.TraditionalWorkQueue

Allowed Values

A Java class that implements or extends the class(es): org.opends.server.api.WorkQueue

Multi-valued

No

Required

Yes

Admin Action Required

Restart the server

Advanced Property

Yes (Use --advanced in interactive mode.)

Read-only

No

max-work-queue-capacity

Description

Specifies the maximum number of queued operations that can be in the work queue at any given time. If the work queue is already full and additional requests are received by the server, then the server front end, and possibly the client, will be blocked until the work queue has available capacity.

Default Value

1000

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

num-worker-threads

Description

Specifies the number of worker threads to be used for processing operations placed in the queue. If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing.

Default Value

Let the server decide.

Allowed Values

An integer value. Lower value is 1. Upper value is 2147483647.

Multi-valued

No

Required

No

Admin Action Required

None

Advanced Property

No

Read-only

No

OpenSolaris Support Reference

Table of Contents

configure

configure — sets the instance location of an OpenDJ package installation

1 Description

The **configure** command configures an OpenDJ package installation. The command registers the directory server as an SMF service, specifies where the directory server instance will be located, and specifies the user and group names of the instance owner.

This command is available in the OpenSolaris™ package installation only.

2 Options

The following options are supported:

`--groupName {groupName}`

The group name of the instance owner. If no group name is specified, the primary group of the *`userName`* is used.

`--instancePath {path}`

The path where the instance will be located. If no path is specified, the default `/var/opendj` is used.

`--userName {userName}`

The user name of the instance owner. If no user name is specified, the default `ldap` is used.

`-V, --version`

Displays directory server version information.

`-?, -H, --help`

Displays usage information.

3 Examples

The following example configures the instance path, user name and group name for a directory server package installation:

```
$ /usr/opendj/configure \
 --instancePath /var/opendj \
 --userName myUser \
 --groupName myGroup
```

4 Attributes

See attributes(5) for descriptions of the following attributes:

opendj

OpenDJ — a high-performance, highly-extensible, LDAPv3 compliant directory server

1 Description

OpenDJ is a high-performance, highly-extensible, pure Java directory server. The server is fully compliant with the LDAPv3 standard, and passes all of the compliance, interoperability and security tests suites. The directory server implements most of the standard and experimental LDAP extensions defined in the IETF as RFCs or Internet-Drafts, ensuring maximum interoperability with LDAP client applications.

OpenDJ software includes a rich set of APIs making the directory server easy to extend. The directory server supports a loosely consistent multi-master replication model that guarantees high availability of data for all operations, searches or updates. While theoretically unlimited with regard to the number of masters, the directory server has been stressed under heavy and durable load with four masters.

OpenDJ software includes:

- A graphical installation tool (**QuickSetup**) that enables you to have a server configured, and up and running in less than 3 minutes
- A graphical control panel (**bin/control-panel**) that displays server status information and enables you to perform basic directory server administration
- A rich set of command-line utilities to perform all online administrative tasks both interactively and with scripts
- Advanced security and password policies
- Advanced backup and restore capabilities
- Extensive user documentation

2 Usage

See the *Installation Guide* for instructions on getting started with OpenDJ directory server.

To install the directory server from IPS packages perform the following steps:

- As the root user, run the **configure** command to create an instance of the directory server in a specific location, running as a specific user.

- Run the **setup** command as this user to install and configure the directory server instance.
- For additional configuration of the directory server, use the **control-panel** and **dsconfig** commands.

Index