

This month's presenters:



Azure Landing Zones

29th January 2025 - External Community Call



Registration:

<https://aka.ms/ALZ/CommunityCall>

Agenda (please add suggestions):

<https://aka.ms/ALZ/CommunityCallAgenda>

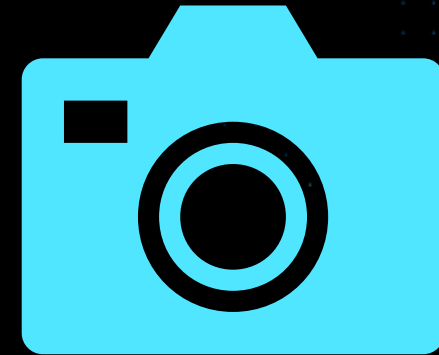
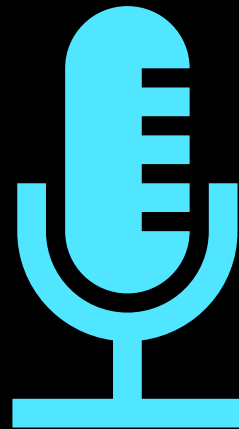
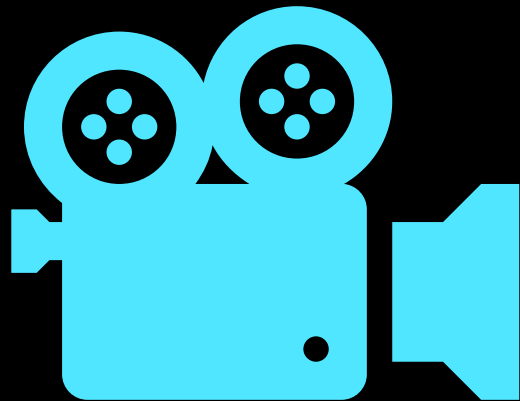




When you join this event, your name, email address and/or phone number may be viewable by other session participants in the attendee list. By joining, you're agreeing to this experience.



Also, this event will be recorded and shared publicly with others, including Microsoft's global customers, partners, employees, and service providers. The recording may include your name and any questions you submit to Q&A.



This meeting is being recorded





Want to hear about the latest Azure Landing Zone events, news, surveys etc.?

If so, sign up to our mailing list:

aka.ms/alz/notifications/signup

Azure Landing Zones -
Notifications - Sign Up



You can also opt out, if registered, by heading to:
aka.ms/alz/notifications/optout

Before we get started...




At any point, if you have a question please put it
in the chat!

(we have members of the team here to help 🧐)


Also we may stop and discuss your
question/point at that time, we want this to be
an open discussion with all of you 😊



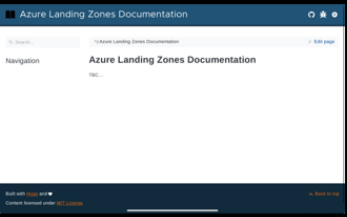




Implementation Options & Accelerators 

ALZ Public Roadmap
aka.ms/ALZ/Roadmap




We shared this last time...




Asks from you  

Portal & Policy Refresh
Q2 FY25 Updates 

AMBA-ALZ Updates
aka.ms/amba/patterns/alz



AzAdvertiser & AzGovViz Updates 


Terraform Azure Verified
Modules for Platform
Landing Zones (ALZ) –
TFAVM4PLZ 


An update on ALZ
features in progress &
upcoming 

Multi-Region Private
DNS for Private Link
A Work In Progress!



A note on upcoming
breaking changes 

Sentinel in ALZ Update 

ALZ + Azure
Connection Program 





Implementation Options & Accelerators



Accelerators



Azure Architecture Center

Browse all Architectures

Architecture icons

What's new

∨ Landing zones

Deployment Options

∨ Design guides

∨ Landing zone implementations

Bicep landing zone implementation

Terraform landing zone implementation

Subscription vending implementation

Cloud operating model roles and responsibilities

The Cloud Adoption Framework describes four common cloud operating models. The Azure identity and access for landing zones recommends five role definitions (Roles) you should consider if your organizations cloud operating model requires customized Role Based Access Control (RBAC). If your organization has more decentralized operations, the Azure built-in roles may be sufficient.

The table below outlines the key roles for each of the cloud operating models.

Role	Decentralized operations	Centralized operations	Enterprise operations	Distributed operations
Azure platform owner (such as the built-in Owner role)	Workload team	Central cloud strategy	Enterprise architect in CCoE	Based on portfolio analysis - see Business alignment and Business commitments
Network management (NetOps)	Workload team	Central IT	Central Networking in CCoE	Central Networking for each distributed team + CCoE
Security operations (SecOps)	Workload team	Security operations center (SOC)	CCoE + SOC	Mixed - see: Define a security strategy
Subscription owner	Workload team	Central IT	Central IT + Application Owners	CCoE + Application Owners
Application owners (DevOps, AppOps)	Workload team	Workload team	Central IT + Application Owners	CCoE + Application Owners

Subscription Vending

Once the platform landing zone is in place, the next step is to create and operationalize application landing zones for workload owners. Subscription democratization is a [design principle](#) of Azure landing zones that uses subscriptions as units of management and scale. This approach accelerates application migrations and new application development.

[Subscription vending](#) standardizes the process for requesting, deploying, and governing subscriptions, enabling application teams to deploy their workloads faster. To get started, see [subscription vending implementation guidance](#), then review the following infrastructure-as-code modules. They provide flexibility to fit your implementation needs.

Deployment option	Description
Bicep Subscription Vending	The Subscription Vending Bicep module is designed to accelerate deployment of the individual landing zones (aka Subscriptions) within an Azure Active Directory Tenant on EA, MCA & MPA billing accounts.
Terraform Subscription Vending	The Subscription Vending Terraform module is designed to accelerate deployment of the individual landing zones (aka Subscriptions) within an Azure Active Directory Tenant on EA, MCA & MPA billing accounts

aka.ms/ALZ/AAC

Platform

The options below provide an opinionated approach to deploy and operate the [Azure landing zone conceptual architecture](#) as detailed in the Cloud Adoption Framework (CAF). It's important to note that, depending upon customizations, the resulting architecture might not be the same for all the options listed below. The differences between the options are how you deploy the architecture. They use differing technologies, take different approaches and are customized differently.

Deployment option	Description
Azure landing zone Portal accelerator	An Azure portal-based deployment that provides a full implementation of the conceptual architecture, along with opinionated configurations for key components such as management groups and policies.
Azure landing zone Terraform accelerator	This accelerator provides an orchestrator module, but also allows you to deploy each capability individually or in part.
Azure landing zone Bicep accelerator	A modular accelerator where each module encapsulates a core capability of the Azure landing zone conceptual architecture . While the modules can be deployed individually, the design proposes the use of orchestrator modules to encapsulate the complexity of deploying different topologies with the modules.

In addition, after deploying the landing zone, you will need to plan to operate it and maintain it. Review the guidance on how to [Keep your Azure landing zone up to date](#).

Application

Application landing zones are one or more subscriptions that are deployed as environments for workloads or applications. These workloads can take advantage of services deployed in platform landing zones. The application landing zones can be centrally managed applications, decentralized workloads, or technology platforms such as Azure Kubernetes Service that host applications.

You can use the options below to deploy and manage applications or workloads in an application landing zone.

Application	Description
AKS landing zone accelerator	An open-source collection of ARM, Bicep, and Terraform templates that represent the strategic design path and target technical state for an Azure Kubernetes Service (AKS) deployment.
Azure App Service landing zone accelerator	Proven recommendations and considerations across both multi-tenant and App Service Environment use cases with a reference implementation for ASEv3-based deployment
Azure API Management landing zone accelerator	Proven recommendations and considerations for deploying APIM management with a reference implementation showcasing App Gateway with internal APIM instance backed Azure Functions as backend.
SAP on Azure landing zone accelerator	Terraform and Ansible templates that accelerate SAP workload deployments using Azure Landing Zone best practices, including the creation of Infrastructure components like Compute, Networking, Storage, Monitoring & build of SAP systems.
HPC landing zone accelerator	An end-to-end HPC cluster solution in Azure using tools like Terraform, Ansible, and Packer. It addresses Azure Landing Zone best practices, including implementing identity, Jump-box access, and autoscale.
Azure VMware Solution landing zone accelerator	ARM, Bicep, and Terraform templates that accelerate VMware deployments, including AVS private cloud, jumpbox, networking, monitoring and add-ons.
Azure Virtual Desktop Landing Zone Accelerator	ARM, Bicep, and Terraform templates that accelerate Azure Virtual Desktop deployments, including creation of host pools, networking, storage, monitoring and add-ons.
Azure Red Hat OpenShift landing zone accelerator	An open source collection of Terraform templates that represent an optimal Azure Red Hat OpenShift (ARO) deployment that is comprised of both Azure and Red Hat resources.
Azure Arc landing zone accelerator for hybrid and multicloud	Arc enabled Servers, Kubernetes, and Arc-enabled SQL Managed Instance see the Jumpstart ArcBox overview.



ALZ Public Roadmap

aka.ms/ALZ/Roadmap

The screenshot shows the 'Azure Landing Zones Public Roadmap' backlog. It is organized into columns based on status: 'We are thinking about...', 'What we are working on...', and 'What we have completed'. Each item is a 'Draft' with associated priority and size tags.

Status	Item	Priority	Size
We are thinking about...	CAF Naming Alignment (ALZ Portal, Terraform, Bicep Implementations)	Low	Large
What we are working on...	Azure Policy Versioning ALZ strategy	High	Medium
What we are working on...	RBAC Constrained Delegation for ALZ	High	Small
What we are working on...	Zone redundancy enhancements	High	Medium
What we are working on...	Multi-region for ALZ	High	Medium
What we have completed	Bicep automation in the ALZ Accelerator	High	X-Large
What we have completed	Subscription vending guidance for common application landing zone vending scenario's	Medium	Medium
What we have completed	MMA Deprecation (MMA --> AMA or Alternatives)	High	X-Large
What we have completed	CAF IAM docs refresh	Medium	Large





ALZ What's New?

aka.ms/ALZ/WhatsNew

🔗 Updates

Here's what's changed in Enterprise Scale/Azure Landing Zones:

🔗 December 2024

🔗 Tooling

- Updated the **Baseline alerts and monitoring** integration section in the portal accelerator to deploy the latest release of AMBA (2024-12-10). To read more on the changes, see the [What's new](#) page in the AMBA documentation.

🔗 November 2024

🔗 Tooling

- A bug was resolved in the Portal Accelerator that caused deployment validation to fail with the error message "The 'location' property must be specified for 'amba-id-amba-prod-001'". This event happened when a Log Analytics Workspace was not deployed, but Azure Monitor Baseline Alerts were enabled. This issue occurred because Azure Monitor Baseline Alerts depend on the management subscription, which is not provided if the Log Analytics Workspace is not deployed. To address this scenario, an additional section was implemented in the Baseline alerts and monitoring tab allowing the selection of a Management subscription when not deploying a Log Analytics Workspace.
- Updated the **Baseline alerts and monitoring** integration section in the portal accelerator to deploy the latest release of AMBA (2024-11-01). To read more on the changes, see the [What's new](#) page in the AMBA documentation.

🔗 Documentation

- Link for the Bicep Subscription Vending changed to AVM (Azure Verified Modules)

🔗 📢 Policy Refresh Q1 FY25

- Updated ALZ custom policies enforcing minimum TLS versions to properly evaluate the minimum TLS version, ensuring services configured to deploy TLS 1.3 will successfully evaluate.
- Updated the initiative [Deploy-MDFC-Config_20240319](#) to the newer version of DCSPM: [Configure Microsoft Defender CSPM plan](#)
- Updated [Deploy-Private-DNS-Generic](#) policy to include the ability to configure the location/region.
- Removed duplicate assignment and portal option of [Deploy Azure Policy Add-on to Azure Kubernetes Service clusters](#) at Landing Zones scope, as this policy is assigned in the initiative [Deploy Microsoft Defender for Cloud configuration](#) at Intermediate Root scope.



CAF What's New?



The screenshot shows the Microsoft Learn website interface. At the top, there's a navigation bar with 'Learn' and several dropdown menus: 'Discover', 'Product documentation', 'Development languages', and 'Topics'. Below that, another navigation bar includes 'Azure' and more dropdowns: 'Products', 'Architecture', 'Develop', 'Learn Azure', 'Troubleshooting', and 'Resources'. A search bar on the left contains the text 'Filter by title'. A sidebar on the left lists various categories under 'Cloud Adoption Framework for Azure', with 'What's new' currently selected. The main content area features the article title 'What's new in the Microsoft Cloud Adoption Framework for Azure' in large white text. Below the title, it indicates 'Article • 07/01/2025 • 34 contributors' and includes a 'Feedback' button. A section titled 'In this article' lists several dates from December 2024 to September 2024, followed by a 'Show 8 more' link. The main text of the article begins with 'We build the Microsoft Cloud Adoption Framework collaboratively with our customers, partners, and internal Microsoft Teams. We release new and updated content for the framework as it becomes available. These new releases pose an opportunity for you to test, validate, and refine the Cloud Adoption Framework guidance along with us.' It concludes with 'Partner with us in our ongoing effort to develop the Cloud Adoption Framework.'



We shared this last time...



The screenshot shows a web page with a dark blue header. The header contains a book icon, the text "Azure Landing Zones Documentation", and three icons: a refresh icon, a share icon, and a settings icon. Below the header is a search bar with the text "Search...", a breadcrumb trail "Azure Landing Zones Documentation", and an "Edit page" link. The main content area has a "Navigation" label on the left, a large heading "Azure Landing Zones Documentation", and the text "TBC...". The footer is dark blue and contains the text "Built with Hugo and ❤️" and "Content licensed under MIT License" on the left, and a "Back to top" link on the right.

📖 Azure Landing Zones Documentation



🔍 Search...

📄 Azure Landing Zones Documentation

✎ Edit page

Navigation

Azure Landing Zones Documentation

TBC...

Built with [Hugo](#) and ❤️

Content licensed under [MIT License](#)

⬆️ [Back to top](#)



And it's becoming a reality...

aka.ms/ALZ/TechDocs



The screenshot shows the Azure Landing Zones Documentation website. The page title is "Azure Landing Zones Documentation". The navigation menu on the left includes sections for Bootstrap, Accelerator, Bicep, Terraform, and Known Issues. The main content area is titled "Azure Landing Zones Documentation" and contains a welcome message, a "Definitions and Concepts" section, and a "The Azure Landing Zones Journey" section. The journey is depicted as a four-step process: Bootstrap your environment, Deploy Azure platform landing zone components, Subscription (LZ) Vending Process, and Deploy workload landing zone components. A flow diagram at the bottom shows the steps: Create Platform Subs, Create Platform, LZ Vending, and Deploy Workload.

Azure Landing Zones Documentation

Welcome to the Azure Landing Zones technical documentation site. This site provides guidance on how to deploy and manage Azure Landing Zones using the solutions we provide.

Use the navigation links on the left to explore the documentation.

Definitions and Concepts

Please see our [documentation on Learn](#) for an introduction to the concepts that we will build on here.

The Azure Landing Zones Journey

The Azure Landing Zones journey is a multi-step process that starts with bootstrapping your environment and ends with the deployment of workloads.

Bootstrap your environment

Whether you're a Brownfield or Greenfield customer, if you're looking to implement a new ALZ environment based on best practices, you'll require multiple subscriptions.

Deploy Azure platform landing zone components

Accelerate the deployment of platform resources based upon ALZ conceptual architecture. Deployment options are available via Azure portal, Terraform and Bicep. They assist with the deployment of management group hierarchy, governance baseline, connectivity, management and security components.

Subscription (LZ) Vending Process

To accelerate the deployment of individual landing zones within an Azure tenant, a subscription vending solution is recommended. Vending helps deploy a subscription and the core resources, e.g., networking. Subscription vending is available using both Terraform and Bicep.

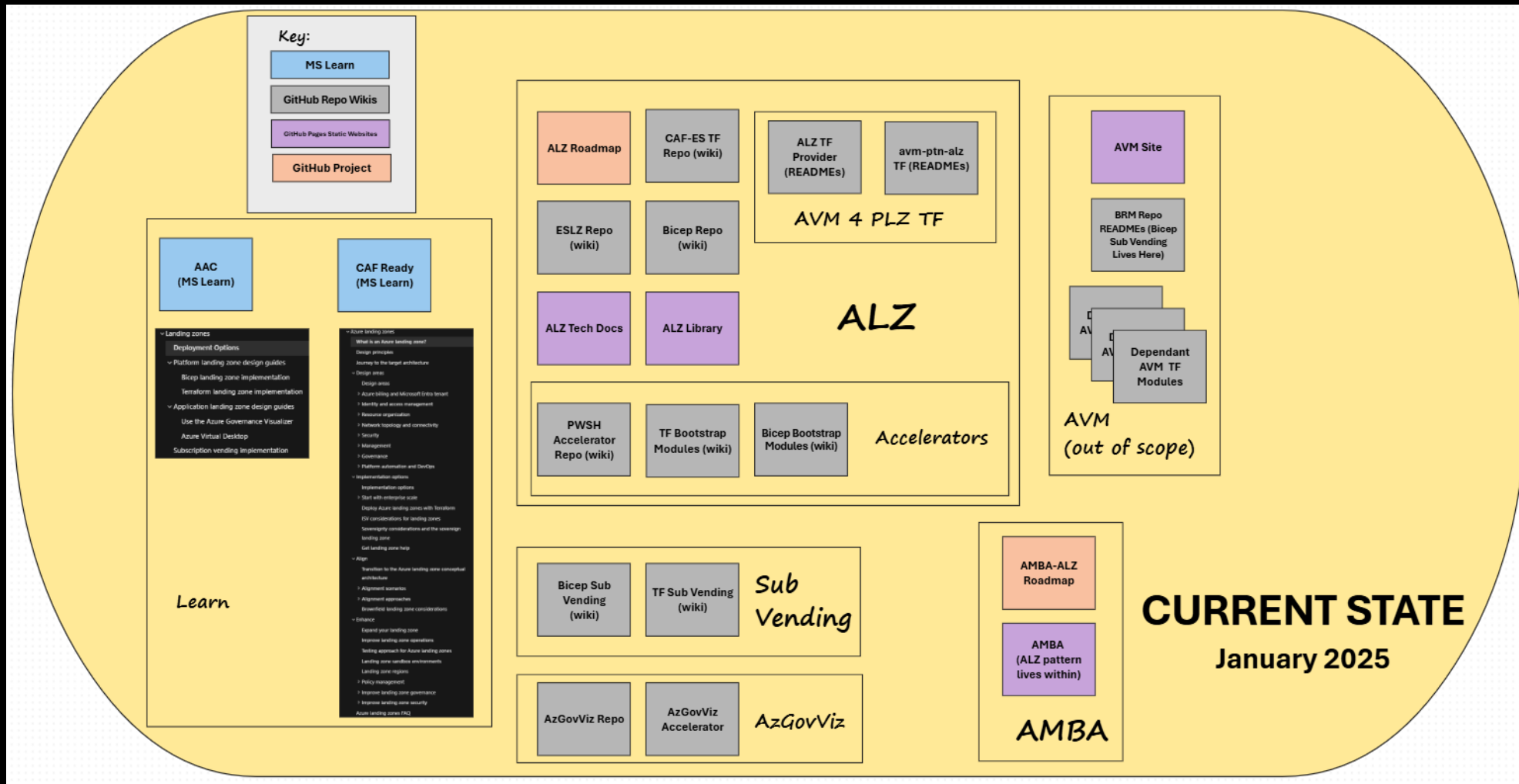
Deploy workload landing zone components

There are multiple Landing Zone accelerators that provide a specific architectural approach and reference implementation for workload scenarios. These accelerators prepare landing zone subscriptions for an enterprise deployments like Azure Virtual Desktop, SAP, AKS etc.. These accelerators are available in a wide range of deployment options.

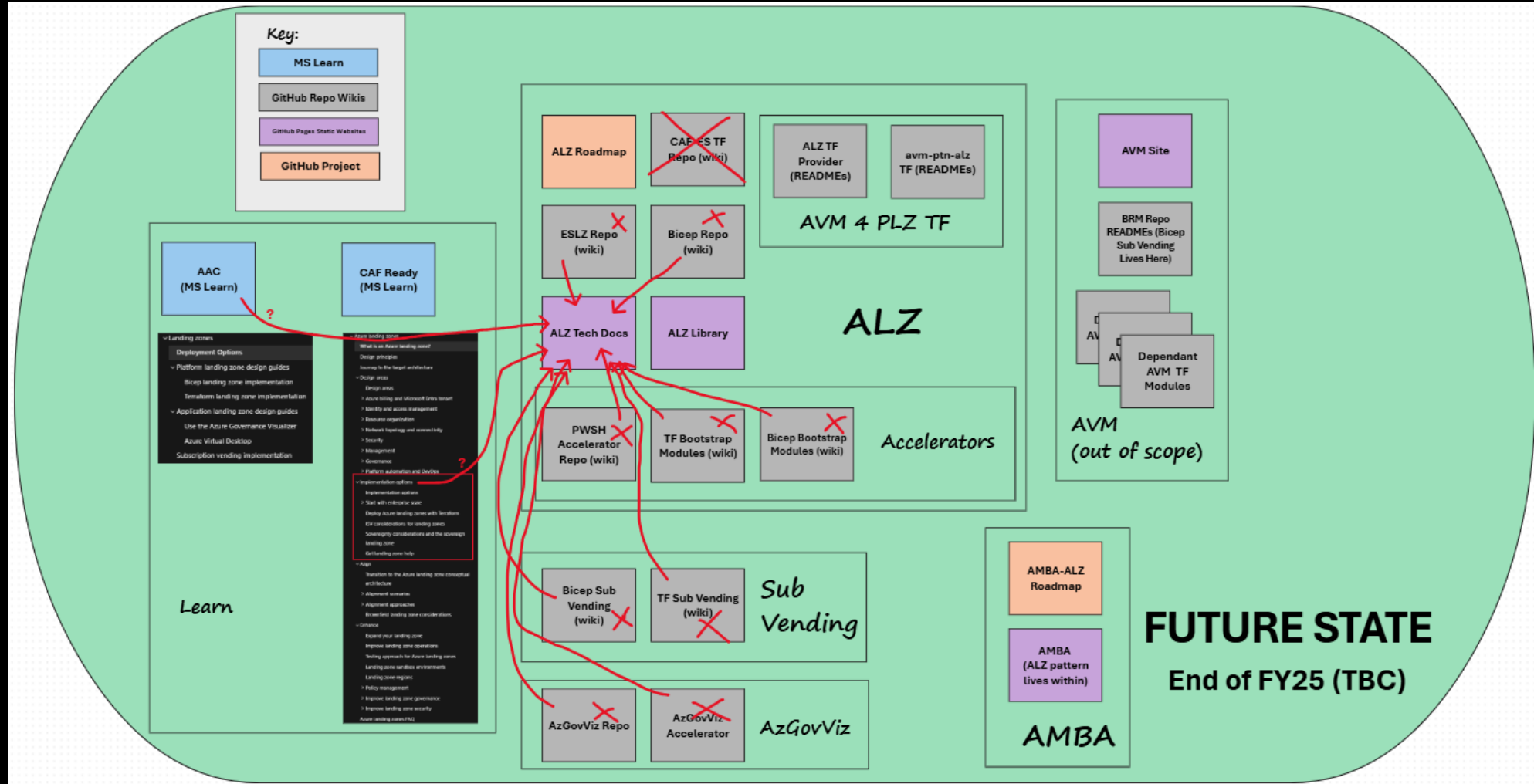
Create Platform Subs → **Create Platform** → **LZ Vending** → **Deploy Workload**



But we aren't stopping there...

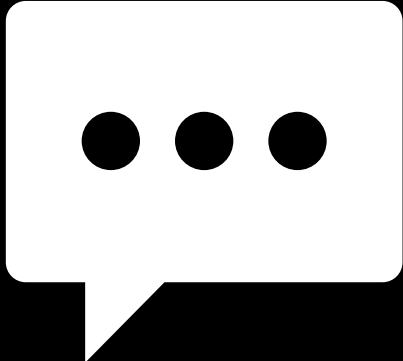


But we aren't stopping there...





Asks from you 🙌





Asks from you 🙋



cjtous1 3 weeks ago

Not sure if this is a bit off-topic, but I would be really interested in having a deep dive on the [azure landing zone library](#).

- What are the possibility for expanding its usage outside the bicep/terraform deployments?
- How to use the alzlibtool
- Building our own libraries
- etc.



4



v1ferrarij 14 minutes ago

Could you please go over the recommendations on using shared resources such as Application Gateways, AKS Clusters, Azure DevOps Agents etc when following the CAF guidelines, where is the recommended place shared resources should live, what Subscription?

I know the recommendation on Application Gateways is to sit within each App LZ, however, we have found a lot of clients are against this due to cost management and would rather have them as a shared resource.

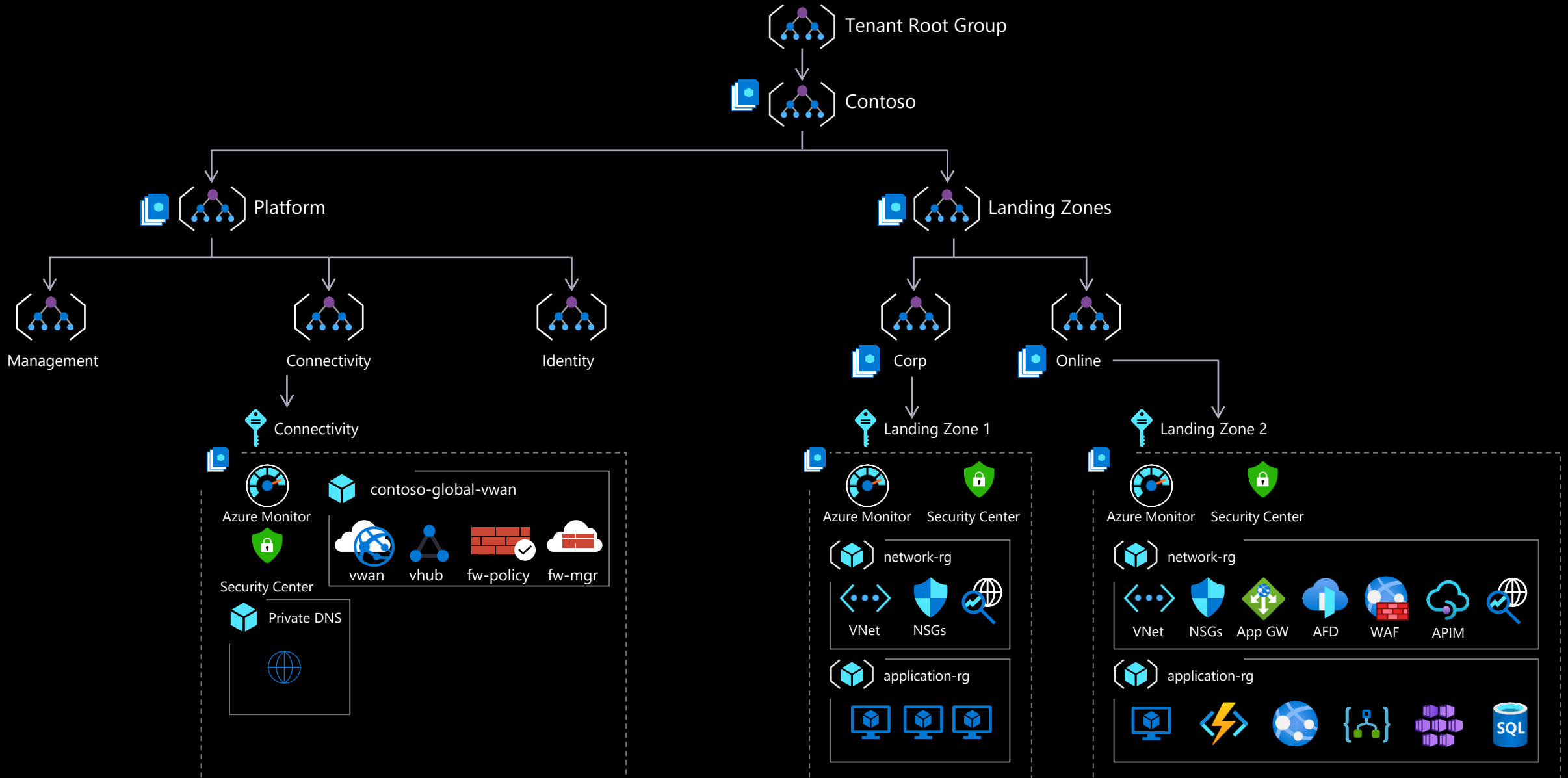
Guidance on this matter would be very beneficial to everyone.



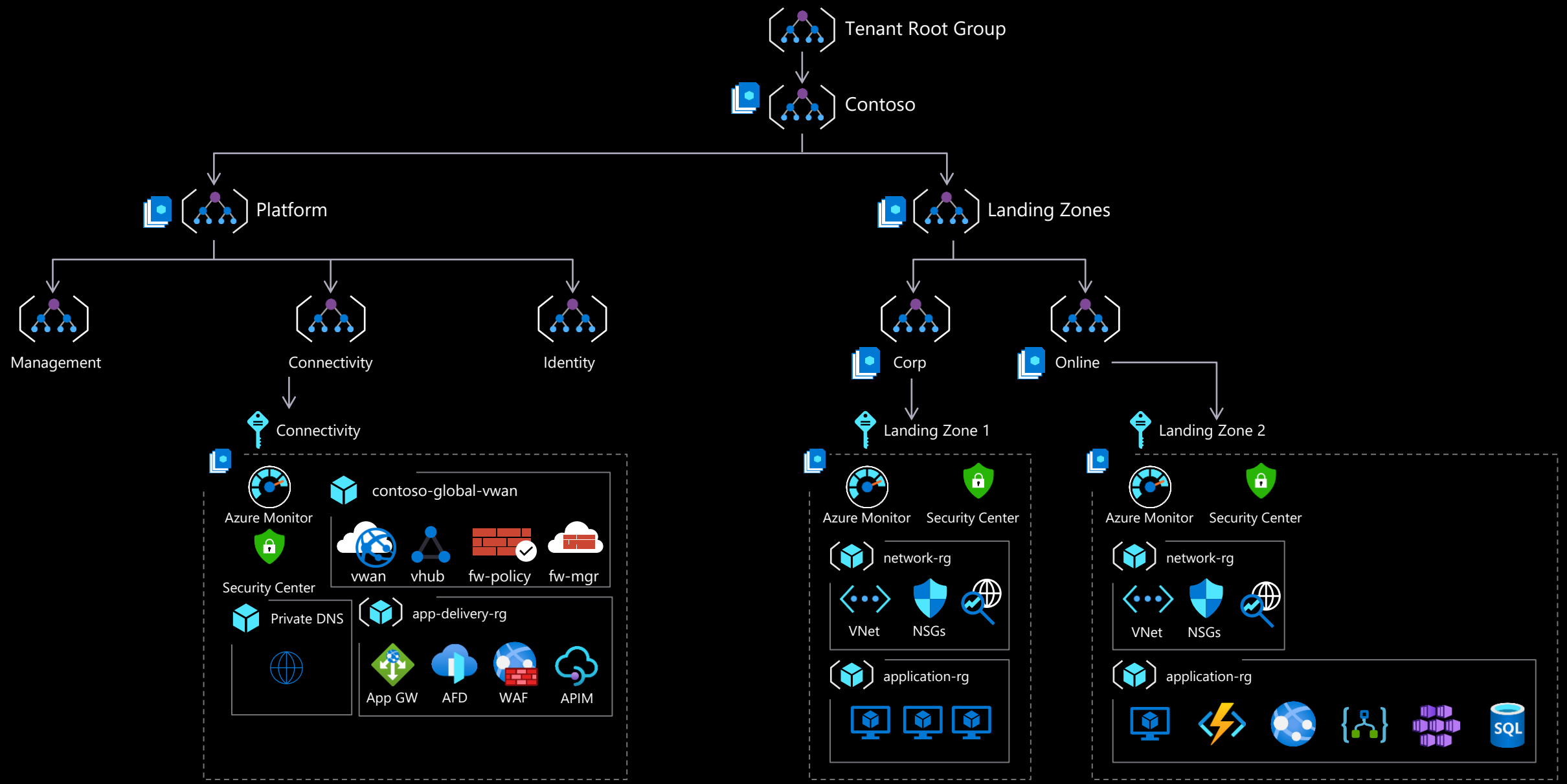
2



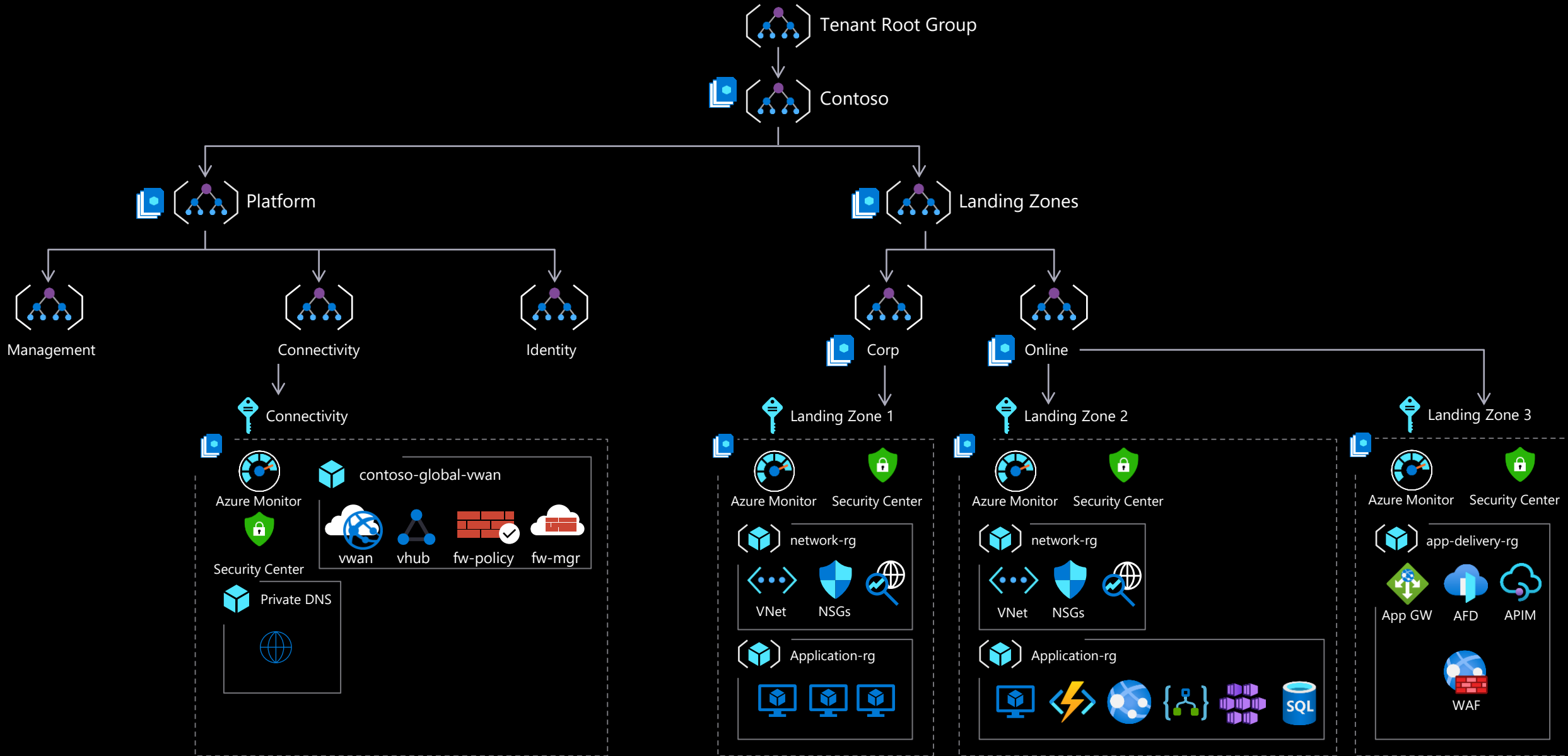
Application Delivery in Landing Zones - Decentralized



Application Delivery in Landing Zones – Centralized Opt. 1

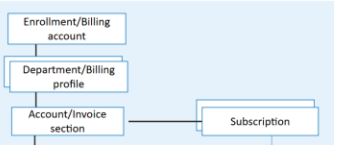


Application Delivery in Landing Zones – Centralized Opt. 2

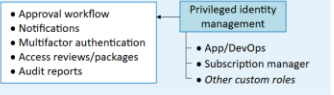




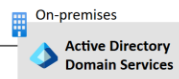
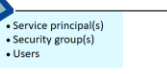
A Enterprise enrollment/Microsoft Customer Agreement



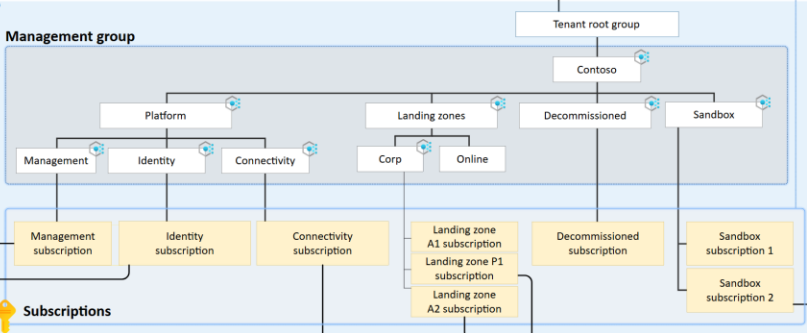
B Identity and access management



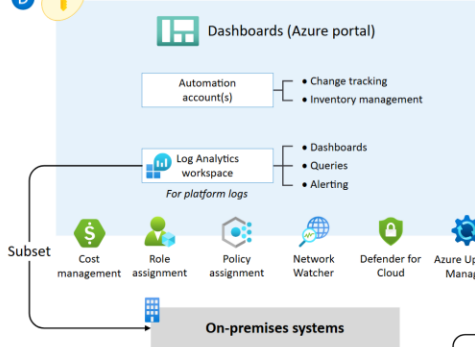
Microsoft Entra ID



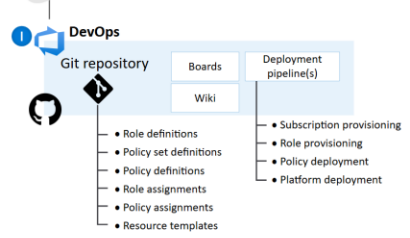
C Management group and subscription organization



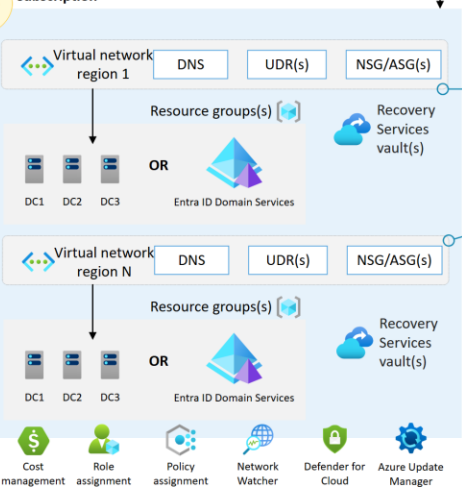
D Management subscription



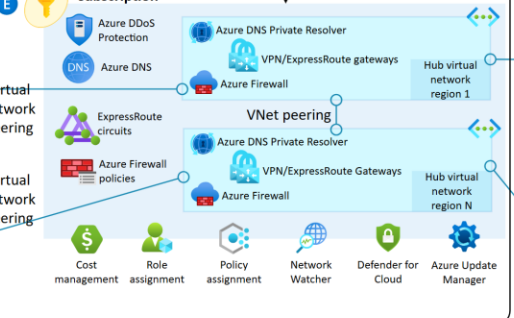
Platform DevOps team



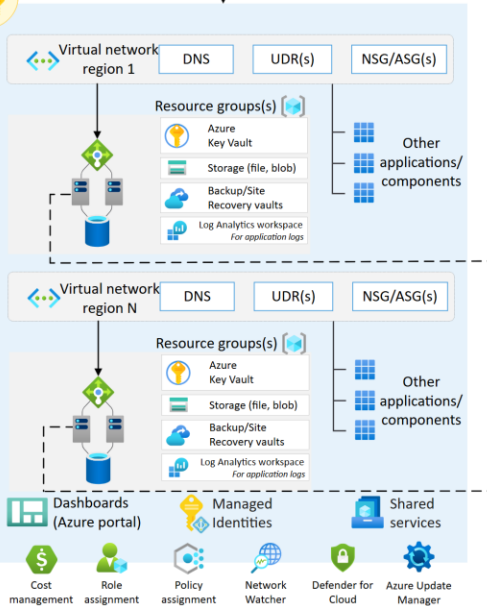
E Identity subscription



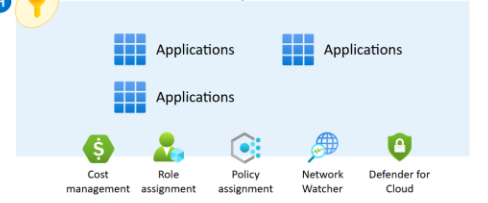
F Connectivity subscription



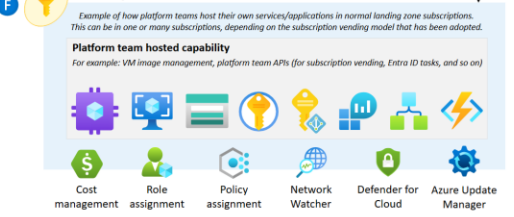
G Landing zone A2 subscription



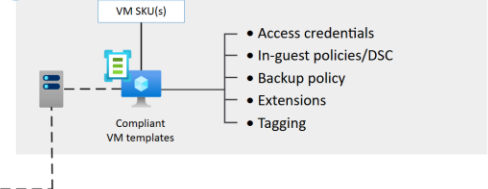
H Sandbox subscription



I Landing zone P1 subscription

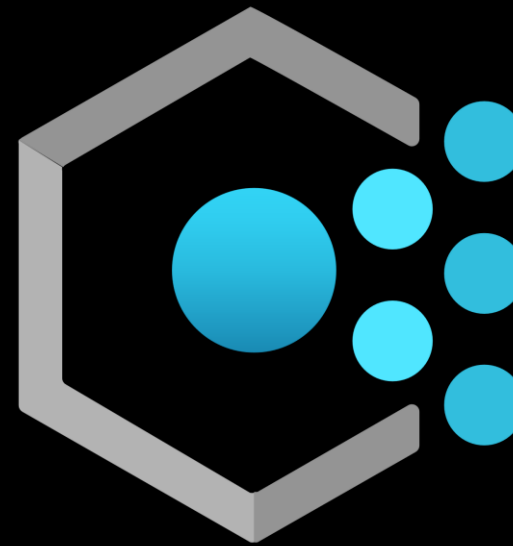


J Compliant VM templates





Portal & Policy Refresh Q2 FY25 Updates





ALZ Policy News

aka.ms/alz/whatsnew



- Policy Refresh Q2 FY25
 - Delayed for several reasons
 - Always review "What's New"
 - One "breaking" change – initiative cleanup
- Policy Versioning
 - Azure Policy Versioning has landed (preview)
 - What has ALZ done?
- General fixes
- Community requests
 - Mandatory Tags (Audit) policies – RG/Resource





ALZ Portal News

aka.ms/alz/portal



- Enhanced pre-requisites and wait logic – drastic reliability improvement for deployments – especially for greenfield
- Azure Virtual Network Manager – Preview
 - Security Admin Rules & blocking high-risk ports from the internet (matching our policy)
- Workload Specific Compliance
 - AI Ready – governance for AI Landing Zones
 - Added "Audit Only" option for all initiatives





AMBA-ALZ Updates

aka.ms/amba/patterns/alz





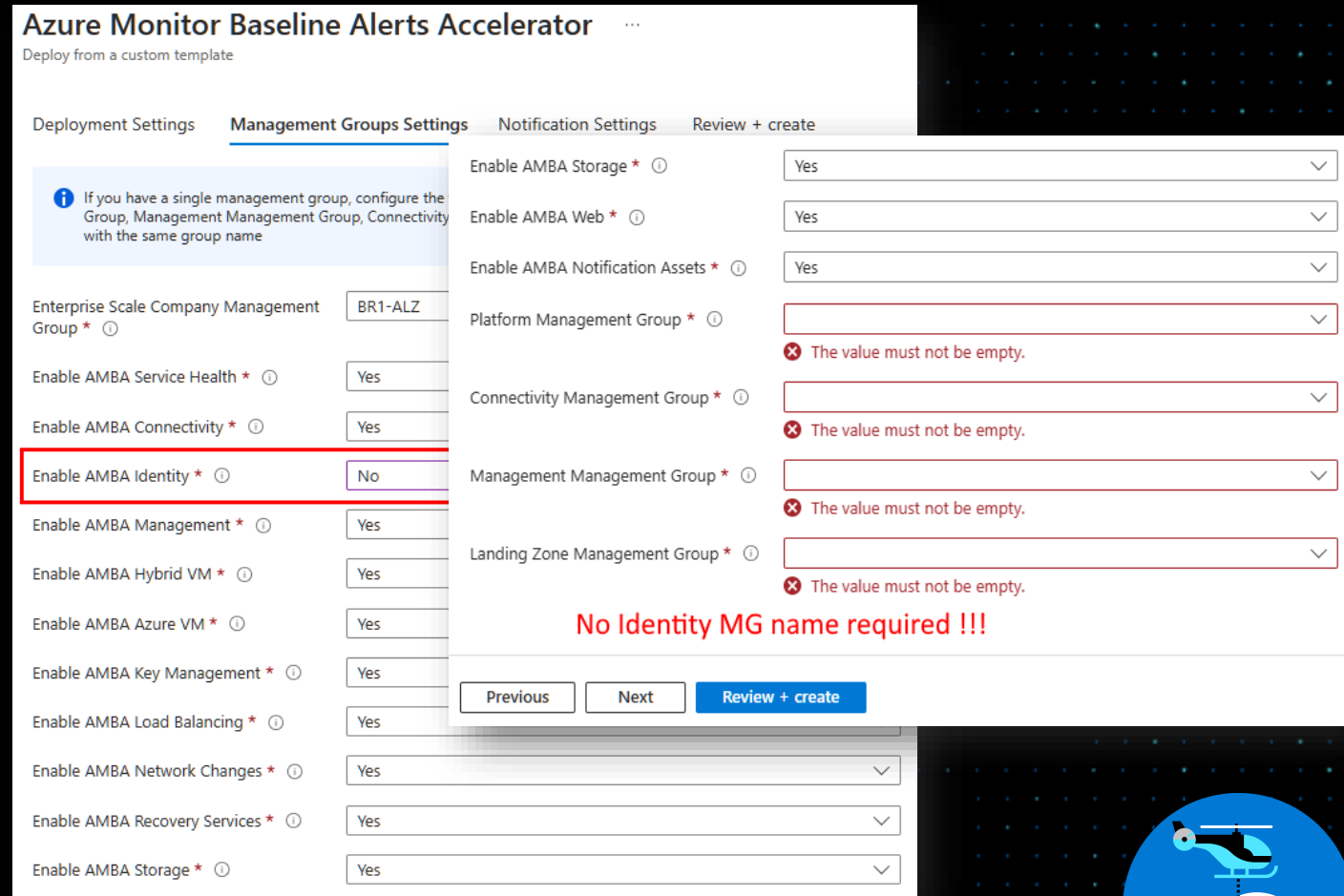
AMBA Updates



aka.ms/amba/alz/whatsnew

- **AMBA-ALZ Portal Accelerator** went GA
(Check the announcement)

- Updated to use the latest AMBA-ALZ release
- Easy filtering of Management Groups and Subscriptions
- Search field to refine the list
- Select what to enable first to enter only scoped info



Azure Monitor Baseline Alerts Accelerator

Deploy from a custom template

Deployment Settings | **Management Groups Settings** | Notification Settings | Review + create

Enable AMBA Identity * No

No Identity MG name required !!!

Review + create



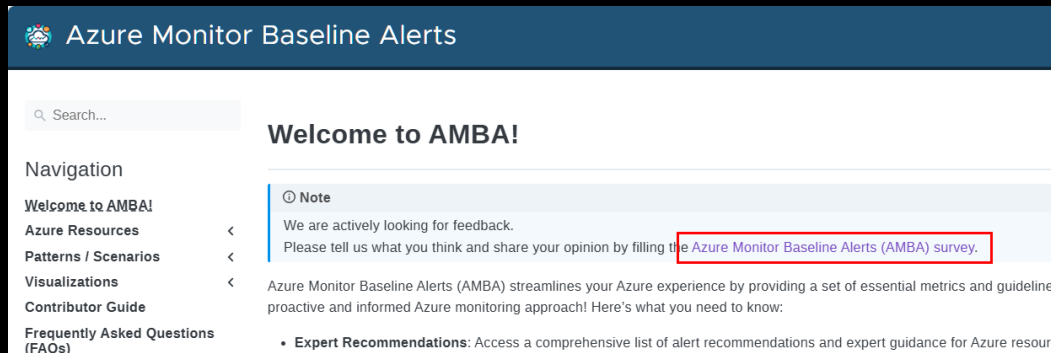


AMBA Updates



aka.ms/amba/alz/whatsnew

- New AMBA survey. Fill it in at aka.ms/ambaSurvey



- **11** bugs fixed
- Maintenance and Remediation scripts consolidation and enhancement with increased robustness

- Faster deployment
- New alerts for:
 - *Application Insights Delete*
 - *Application Insights Throttling Limit reached*
 - *Routes Delete*
 - *Routes Table Delete*
 - *RV ASR Health Monitoring*
- Alert Processing Rule flexibility
- Azure and Hybrid VM policy initiatives assigned to Platform MG
- Documentation Improvement



AMBA Updates

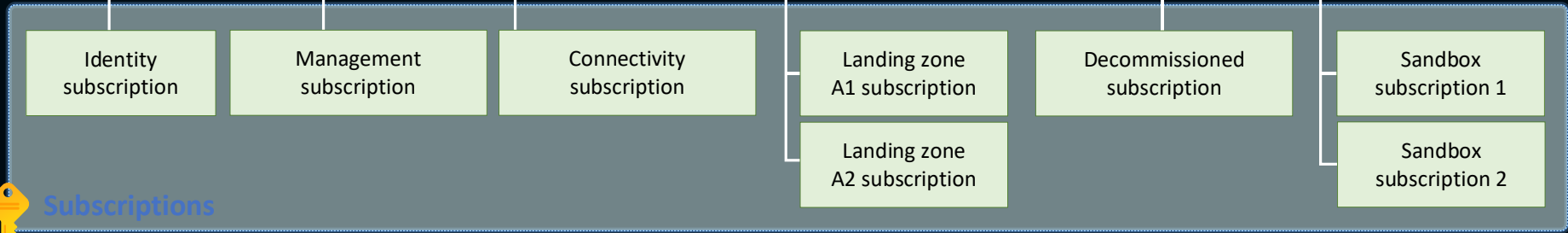
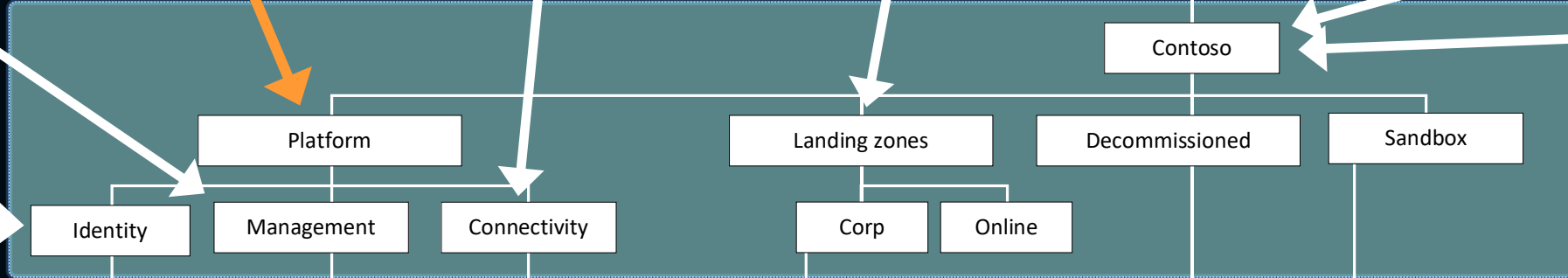
- VM Initiative
- Hybrid Compute

Alerting-Connectivity Initiative

- Key Management Initiative
- Load Balancing Initiative
- Network Changes Initiative
- Recovery Services Initiative
- Storage Initiative
- VM Initiative
- Hybrid Compute
- Web initiative

Management group and subscription organization

Management group




Alerting-ServiceHealth Initiative

Notification Assets Initiative

Alerting-Management Initiative

Alerting-Identity Initiative





AMBA Roadmap

aka.ms/amba/patterns/alz



- Quota Alerts
- AMBA for ALZ Bicep
 - AMBA is not yet integrated into the ALZ-Bicep repository, However, this integration is underway and will soon be available. If you wish to deploy AMBA now, please see this [Wiki](#)
- AMBA for ALZ Terraform
 - We are working on integrating with the Azure-Landing-Zones-Library and updating the module.
- Adding support for CMK for log-alerts storage
- Enabling logical volumes exclusion from disk alerts
- Adding alerts for:
 - Azure Monitor Ingestion limit alert
 - New Resources:
 - Microsoft.Network/virtualhubs (for Route servers)
 - microsoft.network/p2svpngateways
 - Microsoft.Network/routeTables/routes/delete
 - Microsoft.Network/routeTables/delete
- Additional documentation for:
 - Management Groups, Subscriptions, Resource Groups exemption for policy assignment



AzGovViz ALZ Policy Assignments Checker



How to keep up with ALZ policy releases ?

Azure Governance Visualizer | Hide HierarchyMap | Hide TenantSummary | Hide DefinitionInsights | Hide ScopeInsights | Get the latest Azure Governance Visualizer version 6.6.1 (minor) |

HierarchyMap
Hide ScopeInfo
save image

Contoso
MngtPwK2Pm4C127u
remicrosoft.com
207912a0-1574-4a3b-9e4d-29225b6e1e1c

4 37 9
Tenant Root Group
26912a0-1574-4a3b-9e4d-29225b6e1e1c

1 203 2
ALZ

5x

1 2
ALZ-decommissioned

12 8
ALZ-landingzones

1 1
ALZ-platform

4 1 1
ALZ-corp

1 1
ALZ-online

1 1 3 3 1
ALZ-connectivity

1 3 3
ALZ-identity

1 1
ALZ-management

1x

TenantSummary
Policy

- Anything which can help you learn Azure Policy GitHub
- 192 Custom Policy definitions (Tenant wide)
- 42 Orphaned Custom Policy definitions (Tenant wide)
- 51 Custom PolicySet definitions (Tenant wide) (Limit: 51/2500)
- 43 Orphaned Custom PolicySet definitions (Tenant wide)
- 5 custom Policy definition(s) built-in Policy rule parity
- Azure Landing Zones (ALZ) Policy Assignments Checker**
- Azure Landing Zones (ALZ) Policy Version Checker
- 12 Custom PolicySet definitions / deprecated built-in Policy
- 16 Policy assignments / deprecated built-in Policy
- 0 Policy exemptions
- 0 Policy assignments orphaned
- 130 Built-in assignments (43 unique)

Azure Landing Zones (ALZ) Policy Assignments Checker

Azure Landing Zones (ALZ) GitHub | Download CSV semicolon | comma

Rows: 44

ALZ Management Group	Management Group exists / provided	Missing ALZ Policy Assignments	AzAdvertizer Link	ALZ Library release	ALZ release
sandboxes	✖	Enforce-ALZ-Sandbox payload Link	Enforce-ALZ-Sandbox AzA Link	platform/alz/2024.10.1	2024-10-14
connectivity => ALZ-connectivity	✔	Enable-DDoS-VNET payload Link	Enable-DDoS-VNET AzA Link	platform/alz/2024.10.1	2024-10-14
corp => ALZ-corp	✔	Deploy-Private-DNS-Zones payload Link	Deploy-Private-DNS-Zones AzA Link	platform/alz/2024.10.1	2024-10-14
identity => ALZ-identity	✔	Deny-Subnet-Without-Nsg payload Link	Deny-Subnet-Without-Nsg AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deny-IP-forwarding payload Link	Deny-IP-forwarding AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-MDFC-DefSQL-AMA payload Link	Deploy-MDFC-DefSQL-AMA AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-VM-Backup payload Link	Deploy-VM-Backup AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-VM-ChangeTrack payload Link	Deploy-VM-ChangeTrack AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-VM-Monitoring payload Link	Deploy-VM-Monitoring AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-vmArc-ChangeTrack payload Link	Deploy-vmArc-ChangeTrack AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-vmHybr-Monitoring payload Link	Deploy-vmHybr-Monitoring AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-VMSS-ChangeTrack payload Link	Deploy-VMSS-ChangeTrack AzA Link	platform/alz/2024.10.1	2024-10-14
landing_zones => ALZ-landingzones	✔	Deploy-VMSS-Monitoring payload Link	Deploy-VMSS-Monitoring AzA Link	platform/alz/2024.10.1	2024-10-14

Azure / Azure-Landing-Zones-Library

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

7e6b15 - Azure-Landing-Zones-Library / platform / alz / policy_assignments / Enable-DDoS-VNET.alz_policy_assignment.json

```
1 {
2   "type": "Microsoft.Authorization/policyassignments",
3   "subscription": "2812-0b-0e",
4   "name": "Enable-DDoS-VNET",
5   "location": "${default_location}",
6   "dependencies": [],
7   "identity": {
8     "type": "SystemAssigned"
9   },
10  "properties": {
11    "description": "Protect your virtual networks against volumetric and protocol attacks with Azure DDoS Network Protection. For more information, visit https://aka.ms/ddosprotectiondocs.",
12    "displayName": "Virtual networks should be protected by Azure DDoS Network Protection",
13    "policyDefinitions": "providers/Microsoft.Authorization/policydefinitions/94de2a63-ebc1-4caf-ad78-5d479bc83d3d",
14    "enforcementMode": "Default",
15    "parameters": {
16      "ddoSPlan": {
17        "value": "/subscriptions/00000000-0000-0000-000000000000/resourceGroups/placeholder/providers/Microsoft.Network/ddosProtectionPlans/placeholder"
18      },
19      "effect": {
20        "value": "Modify"
21      }
22    },
23    "scope": "providers/Microsoft.Management/managementGroups/placeholder",
24    "notScopes": []
25  }
26 }
```

HOME | POLICY | INITIATIVE | ALIAS | COMPLIANCE | AZURE ACCESS CONTROL | ENTRA-ID ACCESS CONTROL | CATCHUP

AzPolicyAdvertizer

last sync: 2024-Nov-11 18:54:29 UTC

All Azure Policy definitions
Changes on Azure Policy definitions
Track Policy changes in your tenant: Azure Governance Visualizer (aka AzGovViz)

Virtual networks should be protected by Azure DDoS Protection
Azure BuiltIn Policy definition

Source	Azure Portal
Display name	Virtual networks should be protected by Azure DDoS Protection
Id	94de2a63-ebc1-4caf-ad78-5d479bc83d3d
Version	1.0.1 Details on versioning
Versioning	Versions supported for Versioning: 2 1.0.0 1.0.1 Built-in Versioning [Preview]
Category	Network Microsoft Learn
Description	Protect your virtual networks against volumetric and protocol attacks with Azure DDoS Network Protection. For more information, visit https://aka.ms/ddosprotectiondocs.
Mode	Indexed
Type	BuiltIn
Preview	false
Deprecated	false
Effect	Default Modify Allowed Modify, Audit, Disabled

Rbac role(s)

Role Name	Role Id
Network Contributor	4097b08b-164f-4787-a291-c57834212a7

Rule aliases	Id (2)	Alias	Namespace	ResourceType	Path	PathIsDefault	DefaultPath	Modifiable
		Microsoft.Network/virtualNetworks/ddosprotectionplan	Microsoft.Network	virtualNetworks	properties.ddosProtectionPlan	True		True



Terraform Azure Verified Modules for Platform Landing Zones (ALZ) – TFAVM4PLZ 😁



New branding

Terraform Azure Verified Modules for Platform Landing Zones (ALZ)

Composition of Azure Verified Modules

Management

avm-ptn-alz

- Management Groups
- Policy
- Role Definitions

avm-ptn-alz-management

- Log Analytics
- Automation Account

Connectivity

Virtual WAN Option

avm-ptn-virtualwan

- Virtual WAN
- Firewalls

Hub and Spoke Virtual Network Option

avm-ptn-hubnetworking

- Hub Virtual Networks
- Peering
- Firewalls

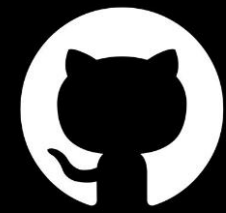
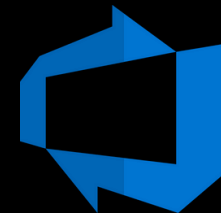
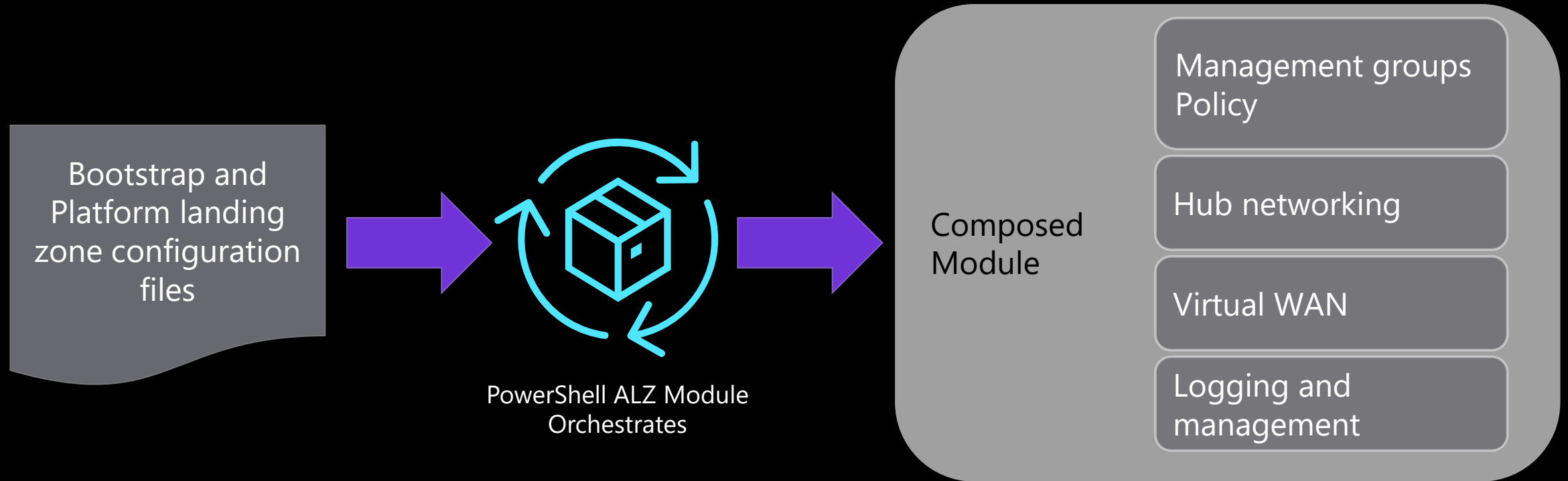
avm-ptn-vnetgateway

- Virtual Network Gateways

avm-ptn-network-private-link-private-dns-zones

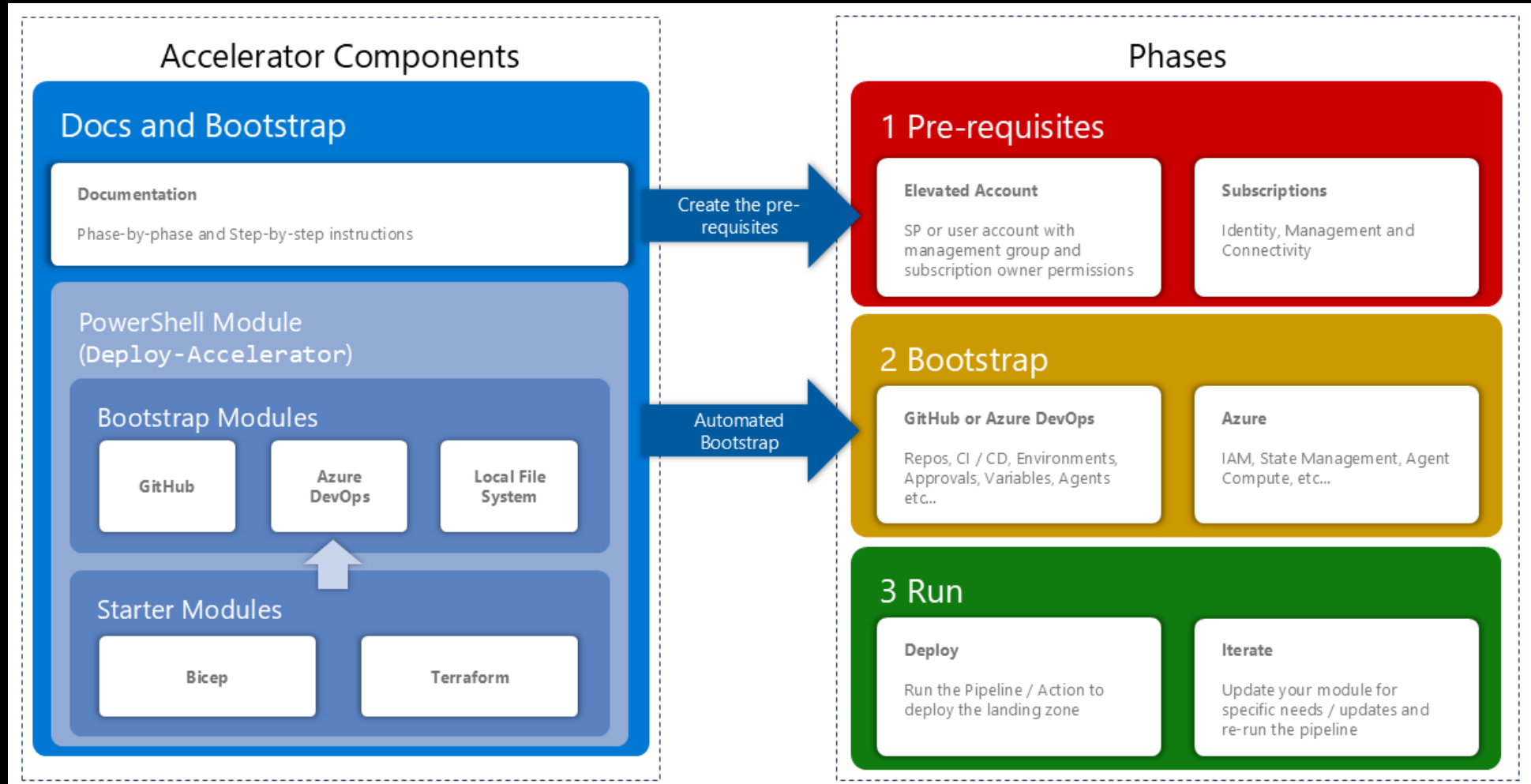
- Private DNS Zones

The ALZ Accelerator – the solution for customers that want a simplified experience



Bootstraps Secure CI / CD

How the ALZ Accelerator Works?



aka.ms/alz/acc

ALZ Accelerator – New Features!

tfvars (HCL) as input for Platform landing zone configuration

- Retains customer updates, formatting, comments and ordering
- Easy to test

Phase 0 – Planning

- Guides you through decisions about bootstrap and Platform landing zone
- Checklist to help record decisions

Options and Scenarios

- Scenarios: 7 high level Platform landing zone architectures
- Options: 14 common customisations

Scenarios

Scenarios are common use cases when deploying the platform landing zone. The following

The available scenarios are:

1. [Multi-Region Hub and Spoke Virtual Network with Azure Firewall](#)
2. [Multi-Region Virtual WAN with Azure Firewall](#)
3. [Multi-Region Hub and Spoke Virtual Network with Network Virtual Appliance \(NVA\)](#)
4. [Multi-Region Virtual WAN with Network Virtual Appliance \(NVA\)](#)
5. [Management Groups, Policy and Management Resources Only](#)
6. [Single-Region Hub and Spoke Virtual Network with Azure Firewall](#)
7. [Single-Region Virtual WAN with Azure Firewall](#)

Options

The available options are:

1. [Customise Resource Names](#)
2. [Customize Management Group Names and IDs](#)
3. [Turn off DDOS protection plan](#)
4. [Turn off Bastion host](#)
5. [Turn off Private DNS zones and Private DNS resolver](#)
6. [Turn off Virtual Network Gateways](#)
7. [Additional Regions](#)
8. [IP Address Ranges](#)
9. [Change a policy assignment enforcement mode](#)
10. [Remove a policy assignment](#)
11. [Turn off Azure Monitoring Agent](#)
12. [Deploy Azure Monitoring Baseline Alerts \(AMBA\)](#)
13. [Turn off Defender Plans](#)
14. [Implement Zero Trust Networking](#)

aka.ms/alz/acc/starter/avm-plz

Rationale



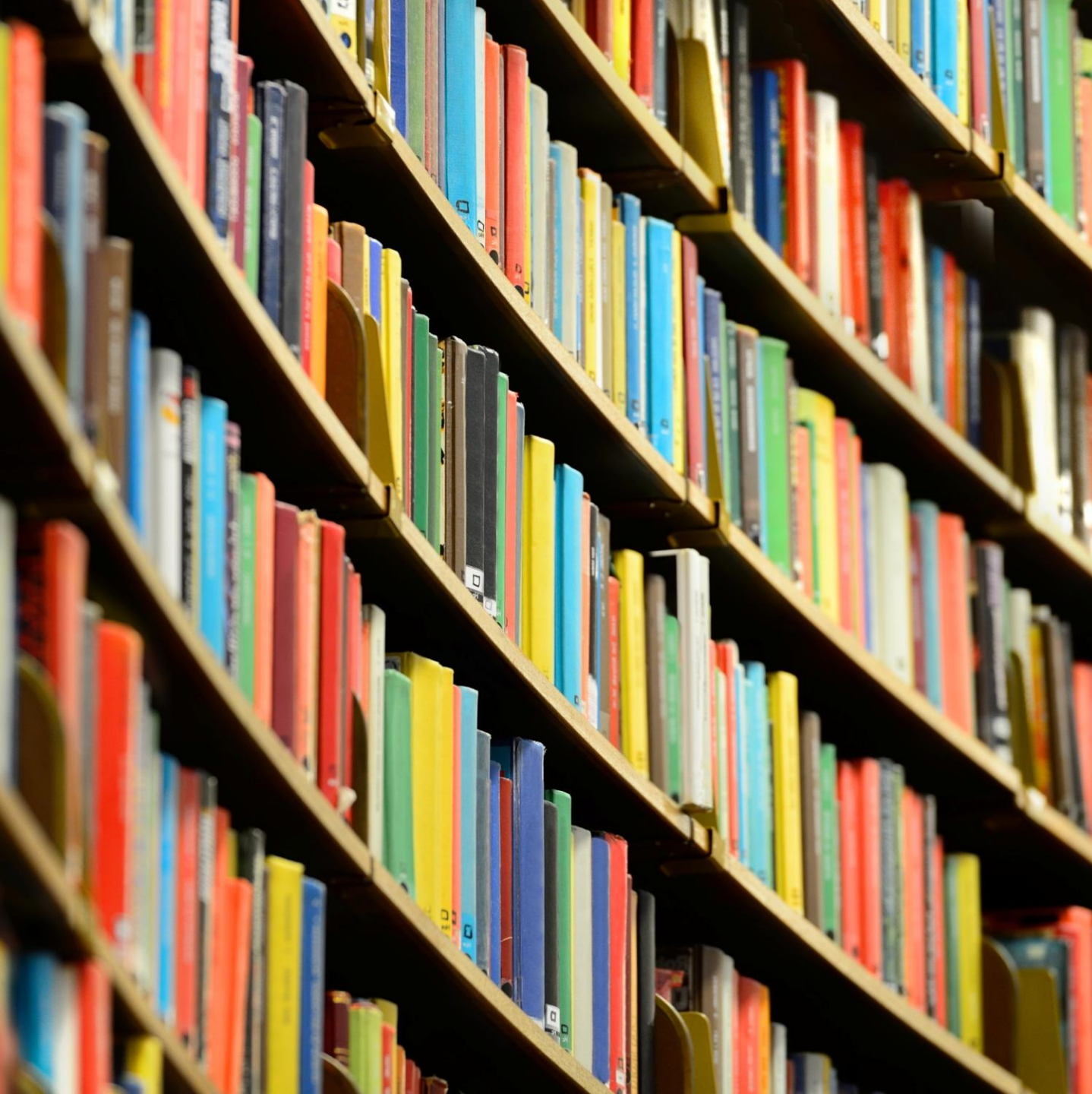
Our largest customers said they wanted a more modular approach



Reaching the limits of what we can do with a Terraform Module (Azure Policy is hard)



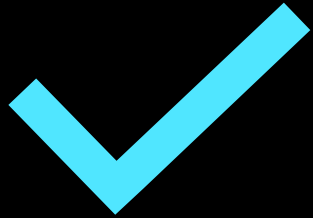
Accelerator provides the same opinionated but configurable approach than the old module, but with the benefit of CI/CD and SCM.



Library

- One source of truth for ALZ, AMBA-ALZ Pattern, etc.
- Hosted in [GitHub Documentation site](#)
- A place to store Azure Landing Zones architectural data, including policies
- Extensible
- Agnostic to the implementation, we plan for the next version of ALZ Bicep to use this as a source

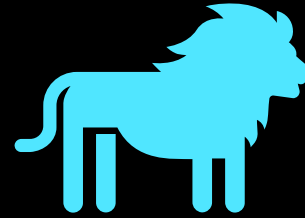
Two approaches



Accelerator

Recommended and supported through the VBD program

Uses the modules that we have produced



Do it yourself

Advanced

Not covered here, [but documented](#)

Here be dragons

Benefits



The provider

Ensures your hierarchy is deployable before you start

Correctly calculates the role assignments required



The Library

Super easy to add AMBA-ALZ, or other additions to your landing zones

Single source of truth for ALZ

Updates decoupled from the module and provider

Automatically generated documentation



The ALZ module

More reliable deployments thanks to retrieable errors

Faster deployments thanks to AzAPI



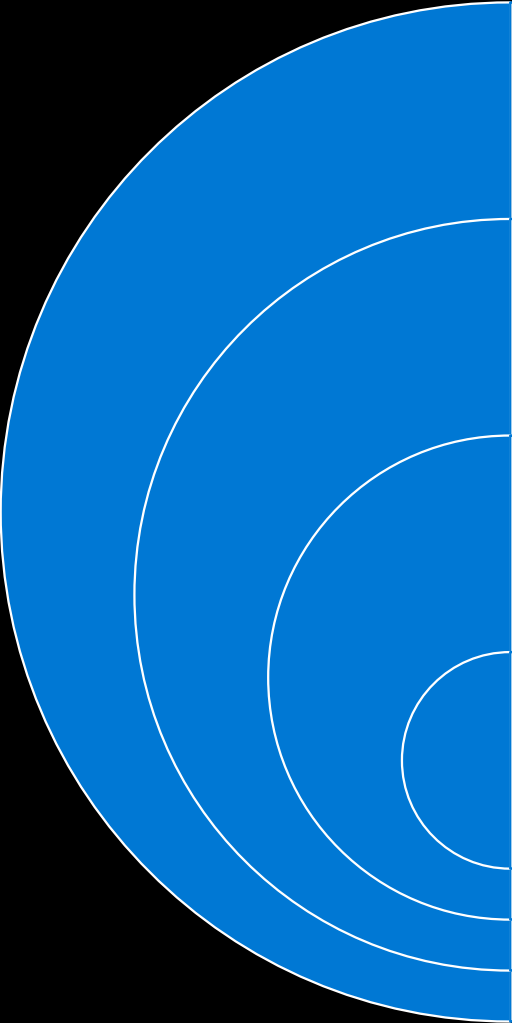
Accelerator

New features:

Bastion

More coming...

Proposed Migration Approach



All subject to testing and validation

Migration will be non-disruptive for all resources

You can continue deploying workloads

Two stages of migration:

- Subscription move to a new management group
- Terraform state migration for management and connectivity resources



ALZ Bicep





ALZ Bicep

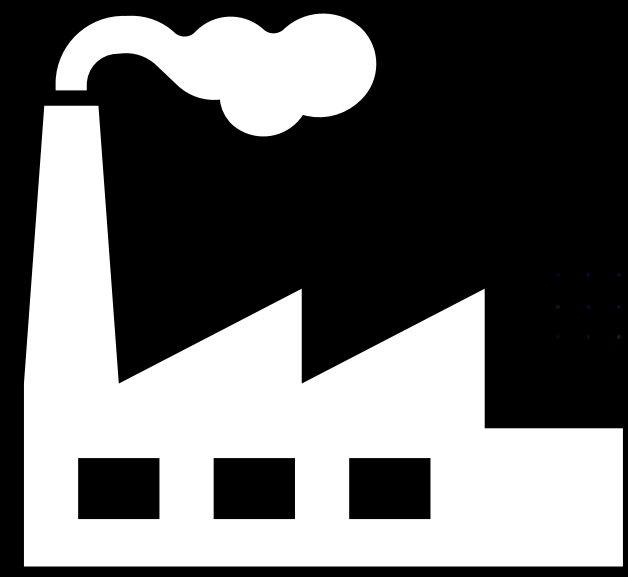


- MVP for [vNext](#): Anticipated for March!
 - We're looking for **teams interested in testing the MVP** before its official launch.
 - ✂ **Scan the QR Code** to sign up and participate!
- ALZ-Bicep (Release of [v0.20.2](#) two weeks ago)
 - Added the option to specify **virtual network gateway IP configuration names**.
 - Added missing **DNS zones** for policy assignment: Deploy-Private-DNS-Zones.
 - Fix role assignments for **AMA Policies**
 - **Az.Resources 7.8.0**
 - Released with **Azure PowerShell v13.1.0**.
 - Resolves the **deployment issue** when using the Accelerator.









An update on ALZ
features in progress &
upcoming






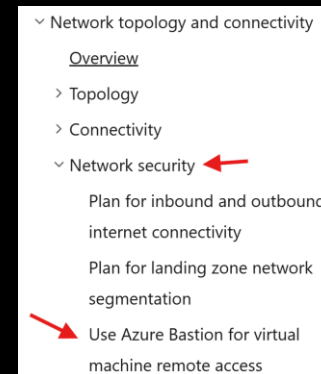
ALZ features alignment progress

Azure Virtual Network Manager (AVNM)

- Security admin rules coming to Portal accelerator 
- [Blog post](#) on envisioning IPAM (IP address management) in ALZ 
- Bicep and Terraform accelerators support 
- Mapping of network groups to ALZ management group hierarchy. Join the [discussion](#) 

Azure Bastion

- New home for Bastion guidance in docs 
- Refreshed guidance for new SKUs 
- Add new SKUs to accelerators + vWan implementation 







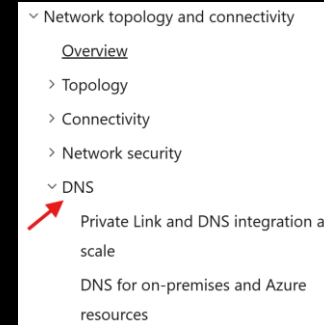
Default VM outbound internet access retirement

- ALZ guidance refresh 
- Ability to deploy NAT gateway in landing zones via Subscription Vending 



ALZ features alignment progress

DNS




- New home for DNS docs 
- Private DNS resolver guidance refresh 
- Private DNS resolver accelerators implementation 
- Multi-Region Private Link Private DNS Guidance Enhancements  (more on this later from Jack)

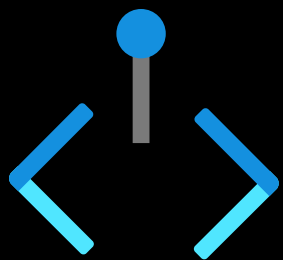


Azure Firewall - Management NIC

- ALZ guidance refresh 
- Accelerators implementation 

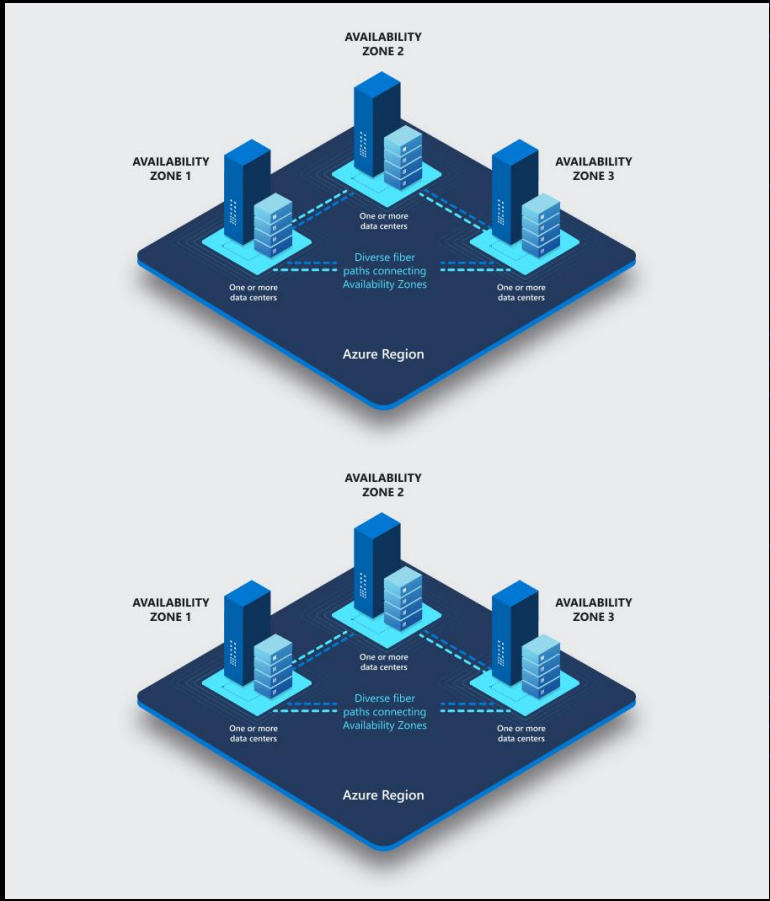
Other networking features


- ExpressRoute Metro guidance 
- Migration of NSG flow logs to Vnet flow logs 
- Subnet peering 



Multi-Region Private DNS for Private Link

A Work In Progress!





This is a complex topic and the ALZ team are sharing their current understanding and thoughts on this important topic.

This is **NOT** official guidance as of today!

A Work In Progress!





Do we deploy a single set of DNS zones centrally in a single region for Private Link?

OR

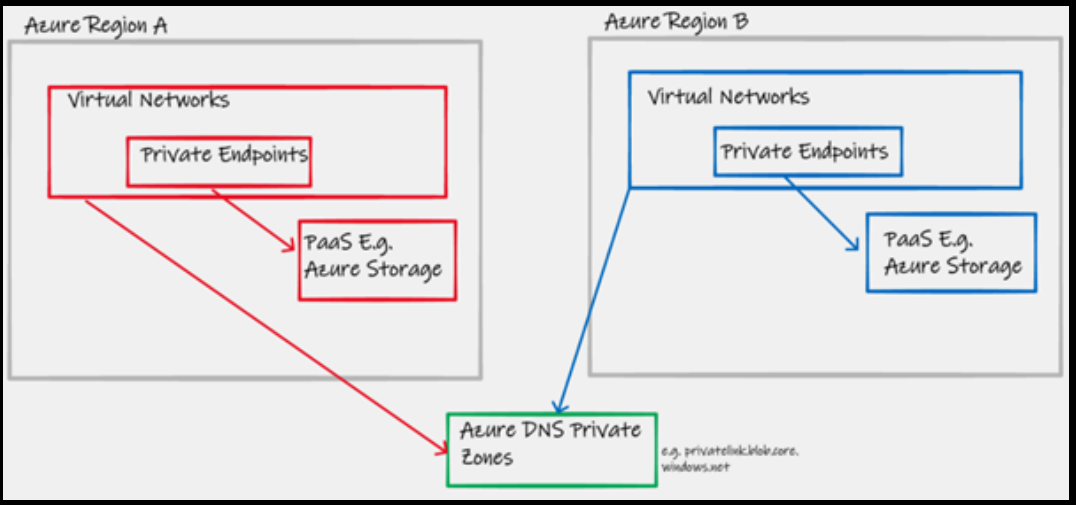
Do we deploy a set DNS zones per-region for Private Link?



A Work In Progress!

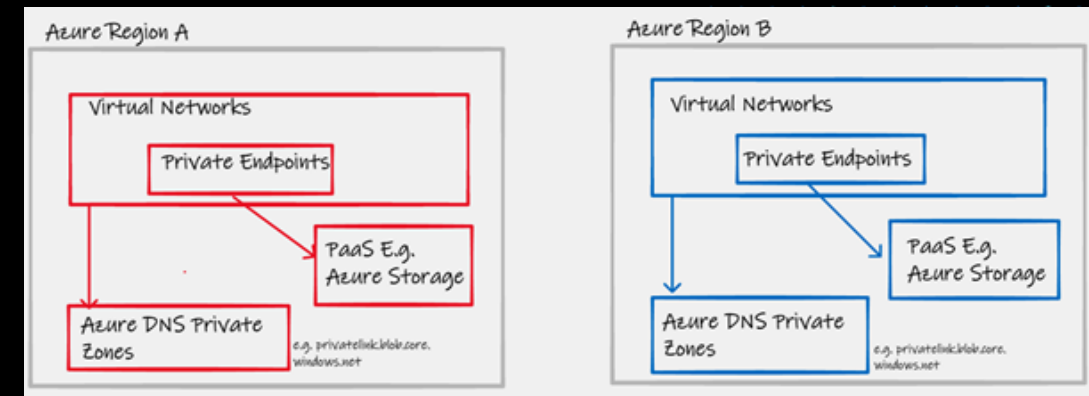


Centralized (single set of zones)



VS

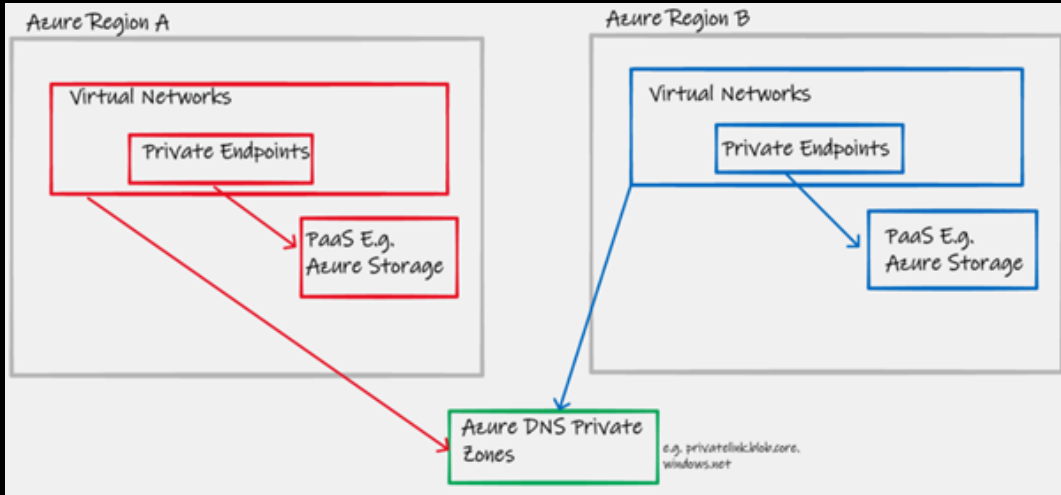
Per-Region (set of zones per-region)



A Work In Progress!

Diagram credits & thought soundboard: Adam Stuart 🙌
 See: github.com/adstuart/azure-privatelink-multiregion

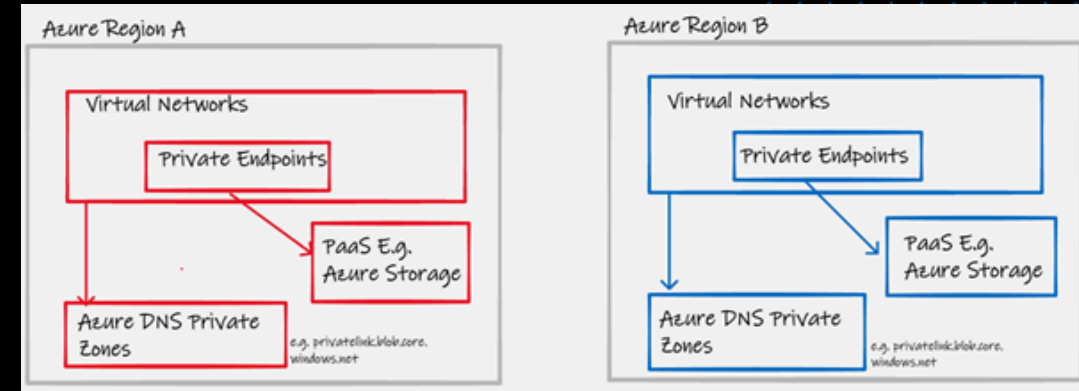
ALZ Recommended Approach **for most**



- Single sets of zones to manage
- Policy automation of DNS Zone Groups works
- Hybrid/On-Premises resolution story is simple
- **Should** be able to update DNS records in region down scenario via REST API call (Terraform, AzCLI, AzPWSH etc.)
 - **NOT** Portal, Bicep, ARM (metadata from RG may be required which prevents these methods)
- No "DNS record syncing system" required
- Not efficient use of SDN
 - Relies on your L3 routing architecture

VS

Only For Advanced Customers **see below for why**



- Multiple sets of zones to manage
- PEs can only have 1 DNS Zone Group for same DNS namespace
 - Forces requirement of "DNS record syncing system" to be built and maintained by **you!**
- Policy automation is complicated (resource selectors etc.)
- Hybrid/On-Premises resolution story is complicated
 - Worse if DNS records are not synced
- PDNS Resolver doesn't let you link same DNS namespaces to single PDNS Resolver instance in single region
 - Makes this approach not feasible ***IMO***
- Efficient use of SDN
- Able to update DNS zone in online region by any method

A Work In Progress!

Diagram credits & thought soundboard: Adam Stuart 🙌
See: github.com/adstuart/azure-privatelink-multiregion





aka.ms/ALZ/MRPLPDNS/Form



We want to hear 🦻 from you 👉, IF:

- You have tackled this problem already today
 - Whether you went single set of global zones or for a set of zones per-region
- Have got a “working” solution today
 - Even if some pain points
- Are considering changing the approach you originally decided upon

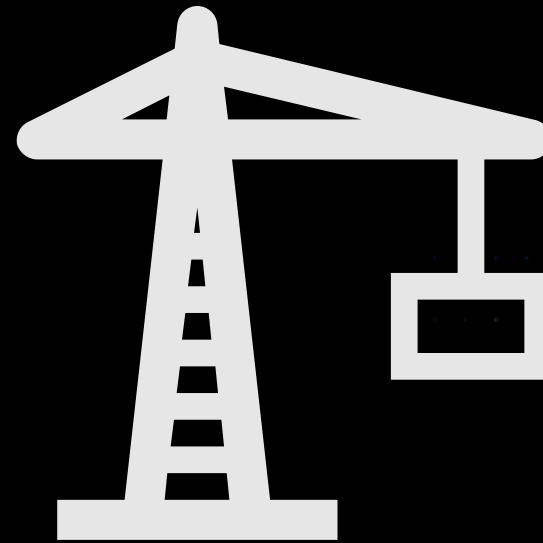
We may reach out to setup some 1-2-1 calls to discuss further to help us shape ALZ guidance and conversations with Product Groups 📞

aka.ms/ALZ/MRPLPDNS/Form





A note on upcoming breaking changes

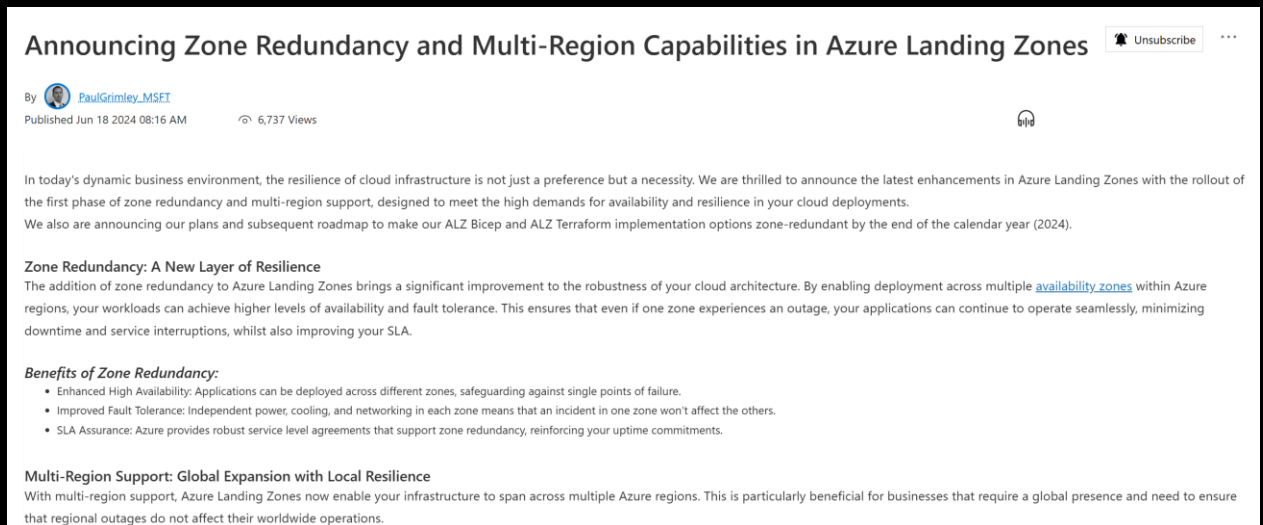





Zone Redundancy Updates



- **BLOG:** Announcing Zone Redundancy and Multi-Region Capabilities in Azure Landing Zones aka.ms/alz/resiliency/blog
- **Phased Approach**
 - ~~Phase 1 – Portal, Bicep and Terraform Accelerators zone redundant by default by end of Q2 CY24~~
 - ~~Phase 2 – Bicep and Terraform Modules zone redundant by default **Early 2025**~~. New Approach – Now planned as part of Migration Tooling & Guidance scheduled for Bicep / Terraform AVM for Platform Landing Zones (ALZ) Modules



Announcing Zone Redundancy and Multi-Region Capabilities in Azure Landing Zones Unsubscribe

By  PaulGrimley_MSET
Published Jun 18 2024 08:16 AM 6,737 Views

In today's dynamic business environment, the resilience of cloud infrastructure is not just a preference but a necessity. We are thrilled to announce the latest enhancements in Azure Landing Zones with the rollout of the first phase of zone redundancy and multi-region support, designed to meet the high demands for availability and resilience in your cloud deployments. We also are announcing our plans and subsequent roadmap to make our ALZ Bicep and ALZ Terraform implementation options zone-redundant by the end of the calendar year (2024).

Zone Redundancy: A New Layer of Resilience
The addition of zone redundancy to Azure Landing Zones brings a significant improvement to the robustness of your cloud architecture. By enabling deployment across multiple [availability zones](#) within Azure regions, your workloads can achieve higher levels of availability and fault tolerance. This ensures that even if one zone experiences an outage, your applications can continue to operate seamlessly, minimizing downtime and service interruptions, whilst also improving your SLA.

Benefits of Zone Redundancy:

- **Enhanced High Availability:** Applications can be deployed across different zones, safeguarding against single points of failure.
- **Improved Fault Tolerance:** Independent power, cooling, and networking in each zone means that an incident in one zone won't affect the others.
- **SLA Assurance:** Azure provides robust service level agreements that support zone redundancy, reinforcing your uptime commitments.

Multi-Region Support: Global Expansion with Local Resilience
With multi-region support, Azure Landing Zones now enable your infrastructure to span across multiple Azure regions. This is particularly beneficial for businesses that require a global presence and need to ensure that regional outages do not affect their worldwide operations.





Sentinel in ALZ Update



We have been looking into this...



ALZ Requirement Specification



Security Subscription with Sentinel Deployment

Author:

Status: Draft

1. Problem statement

Customers deploy their Microsoft Sentinel implementations after their landing zones using a variety of methods, or as part of their Azure Landing Zone deployment. When they do so, they are often taking the path of least resistance. This means they often deploy Sentinel to the Log Analytics Workspace associated with the ALZ Management Subscription. This might be done by the customer themselves, or it might be done by Microsoft team members who are focused on getting Sentinel up quickly as part of executing VBDs or other engagements.

However, this LAW has more logs than are needed. It contains a variety of management logs that are not required for Sentinel's security operations. When customers deploy Sentinel to this LAW, they take on a significant cost burden without additional value.

Today customers can use the Azure Sentinel All-in-One for the deployment: [Azure-Sentinel/Tools/Sentinel-All-in-One at master · Azure/Azure-Sentinel \(github.com\)](#). This package deploys out a new LAW, and configures Microsoft Sentinel. However, it doesn't enforce the use of a dedicated Security Subscription.

2. Justification

Sentinel deployments are often deployed in a subscription with many elevated permissions. Due to Sentinel's critical nature, it should be in an isolated subscription. A subscription is a security boundary with its own Control Plane (Identity/RBAC). This will give you the opportunity to isolate Sentinel from other resources and scope creep. An owner of a Subscription will inherit Sentinel ownership so if Sentinel is in a subscription for application development you can expect that the owner of that will have access. There are other methods of reducing this creep, but a separate subscription is the easiest. A subscription itself doesn't incur charges. It's the resources within that cost money.

Cost is the second driver. Once customers realize that they have taken on this cost burden, they become dissatisfied and often need assistance in remediating and redeploying Sentinel. This places effort on Microsoft and on the customer, as well as further reducing their satisfaction with the products and delaying other initiatives. This dissatisfaction is heightened if the deployment was done by Microsoft team members.

We can ensure charge back on Sentinel based on consumption in the one subscription. Sentinels have peripheral objects like Logic Apps, Function Apps and Machine Learning that have costs associated with them as well.

The best way to address the subscription assignment and LAW location is by including the correct configuration where possible, and to enforce good practices through policies.

3. Success Measurement

Success measurements include:

- Reduced number of satisfaction calls due to Sentinel charges.

MICROSOFT CONFIDENTIAL

-1-

ALZ Requirement Specification



- Specific case testing to confirm that customers cannot accidentally deploy a Sentinel instance to the Management LAW.

4. Functional Requirements

Automation driving Customer to deploy the pattern we want

Policy denying the behavior we do not want.

Documentation explaining what needs to happen.

No.	Requirement	Priority
SE-F1	When deploying the ALZ Portal reference implementation, customers should be prompted with an option to deploy Azure Sentinel. If selected, the customer will be prompted to select a subscription for the deployment – the Security Subscription. When the ARM templates are deployed with these options selected, a Management Group deployment will deploy a Security Management Group that is a child of the Platform Management Group, and place the Security Subscription in it. It will then deploy a Resource Group, a Log Analytics Workspace, and Sentinel. There should also be logic to check the 4 platform subscriptions are not the same for security, management, connectivity and identity, if possible.	
SE-F2	Diagrams for Landing Zones should include the Security management group and subscription. Locations include: Azure landing zone design areas - Cloud Adoption Framework Microsoft Learn	
SE-F3	In the Security Design Area, a new article for Sentinel needs to be defined, with the topics of: <ul style="list-style-type: none">Planning your Sentinel deploymentRecommendations & ConsiderationsLink to deployment tools	
SE-F4	When deploying with Terraform, there should be a parameter and module set that can be used to trigger the creation of a Security Management Group, Sentinel Resource Group, LAW, and Sentinel instance. This will require adding new parameters, including one for the Security Subscription.	
SE-F5	When deploying with Bicep, there should be a parameter and module set that can be used to trigger the creation of a Security Management Group, Sentinel Resource Group, LAW, and Sentinel instance. This will require adding new parameters, including one for the Security Subscription.	
SE-F6	Policies should be assigned to the Management management group that deny the deployment of Sentinel to enforce best practices.	
SE-F7	If SE-F4, SE-4, or SE-5 are used by a customer, an initiative for Sentinel logs should be created and assigned to the Landing Zone management group. The policies would include common resource types provided by the Product Groups. This should be like the existing "Deploy-Diag-Logs" initiative and the "Deploy Diagnostic Settings for Activity Log to Log Analytics workspace" initiative, but with a different Log Analytics selected and a different scope of content.	

MICROSOFT CONFIDENTIAL

-2-

ALZ Requirement Specification



5. Non-functional Requirements (Fundamentals)

No.	Requirement	Priority
SE-NF1	Prevent customers from deploying Microsoft Sentinel to the Log Analytics Workspace in the Platform Management subscription.	
SE-NF2	Guide customers to deploy Microsoft Sentinel in a dedicated subscription, with a dedicated Log Analytics Workspace.	
SE-NF3	Empower customers to deploy Microsoft Sentinel as part of Azure Landing Zones.	
SE-NF4	Capture telemetry on customer deployments of Microsoft Sentinel as part of Azure Landing Zones.	

6. Spec History

[Once the spec is available for review, capture the date and reason for every change to the specification]

Date	Changes Made	Author
------	--------------	--------

7. Optional Sections

[Refer to the [Requirements Specification wiki article](#) for possible additional sections for this specification.]

MICROSOFT CONFIDENTIAL

-3-





Decisions to make...



Do we need a separate LAW dedicated to Sentinel?

- We think so, mainly due to platform logs increasing costs and causing noise from required security logs
 - Even though this will lead to some double logging into both LAWs (Platform + Sentinel)
- Often organizations have separate Security teams requesting/driving for this
- Product Group guidance leans to single workspace by default, see [here](#).

Do we need a separate "Security" platform Subscription?

- Can it not just live in Management?

Does this need to be in a separate "Security" Management Group?

- Could it just live inside of Platform > Management?
 - Does it need to be somewhere else?
- RBAC is suggested to be done at Subscription scope, not MG.
 - MGs are primarily for policy assignments

Should ALZ deploy anything Sentinel related? Or should we just provide placement guidance and platform pre-reqs?

- e.g. Should we just deploy and move a subscription to a management group that ALZ creates?
- This then allows security teams to deploy and manage sentinel however they wish
 - Also, they then work with the ALZ/Platform team to get any additional RBAC and policy assignments created as they see fit?
- Or should ALZ deploy [Sentinel All-In-One Accelerator](#), or just provide guidance and link to it?



We want to hear  from you 

aka.ms/ALZ/SentinelFuture



Azure / Enterprise-Scale

Code Issues 88 Pull requests 9 Discussions Actions Projects 1 Wiki Security 42 Insights Settings

The future of Sentinel in ALZ (follow on from 29th January 2025 Community Call) #1898

Unanswered jtracey93 asked this question in Ideas

jtracey93 4 minutes ago Maintainer

As you have heard or seen in the community call on 29th January 2025 we are considering the future of Sentinel in ALZ and whether we need to change the architecture or not.

We are looking for your input on what you are doing or seeing in the wild today, to help shape the changes to ALZ (if required) so it is based on real-world deployments 🚀

Decisions to make...

- Do we need a separate LAW dedicated to Sentinel?**
 - We think so, mainly due to platform logs increasing costs and causing noise from required security logs
 - Even though this will lead to some double-logging into both LAWs (Platform + Sentinel)
 - Other organizations have separate Security teams requesting/driving for this
 - Product Group guidance leans to single workspace by default, see [here](#)
- Do we need a separate "Security" platform Subscription?**
 - Can it not just live in Management?
- Does this need to be in a separate "Security" Management Group?**
 - Could it just live inside of Platform + Management?
 - Does it need to be somewhere else?
 - RBAC is suggested to be done at Subscription scope, not MG.
 - MGs are primarily for policy assignments.
- Should ALZ deploy anything Sentinel related? Or should we just provide placement guidance and platform pre-req?**
 - e.g. Should we just deploy and move a subscription to a management group that ALZ created?
 - This then allows security teams to deploy and manage sentinel however they wish
 - Also, they then work with the ALZ/Platform team to get any additional RBAC and policy assignments created as they see fit?
 - Or should ALZ deploy Sentinel all in One Accounts, and just provide guidance and link to it?

Questions to answer (we want to hear from you 🗣️ - reply in the comments below)

1. Do we need a separate LAW dedicated to Sentinel?
 - 1. We think so, mainly due to platform logs increasing costs and causing noise from required security logs

Category: Ideas

Labels: Area: Logging & Aut..., Needs: More Evidenc..., Status: Help Wanted..., Type: Enhancement..., Type: Feature Reque...

1 participant

Notifications: Unsubscribe

You're receiving notifications because you're watching this repository.

Lock conversation, Transfer this discussion, Pin discussion, Pin discussion to Ideas, Create issue from discussion, Delete discussion





ALZ + Azure Connection Program





ALZ Influencers Group (Pilot)



- **Purpose**

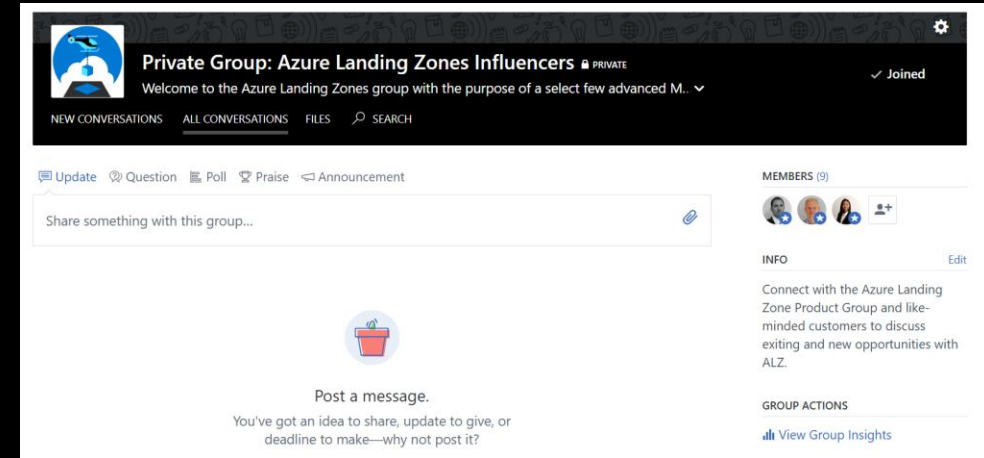
- Gain insights from trusted group
- Two-way communication
- **NOTE: Not intended as a support channel – continue to use GitHub Issues**
- **Not linked to MVP Program!**

- **Criteria**

- Previously Contributed
- Are you an ALZ ambassador? Do you Promote ALZ?
- See yourself as an ALZ expert?

- **Complete link**

- **Triage applications, no guarantees on entry (we'll only choose a few to start)**



5. What areas of ALZ are you an "expert" in? *

- Billing & Entra ID Tenant
- IAM
- Resource Organization
- Networking
- Security
- Management
- Governance
- Platform Automation & DevOps
- Bicep
- Terraform
- Portal
- Accelerator

aka.ms/alz/influencers/nominate





Azure Landing Zones

7th May 2025 - External Community Call



Registration:

aka.ms/ALZ/CommunityCallRegister

Agenda (please add suggestions):

aka.ms/ALZ/CommunityCallAgenda

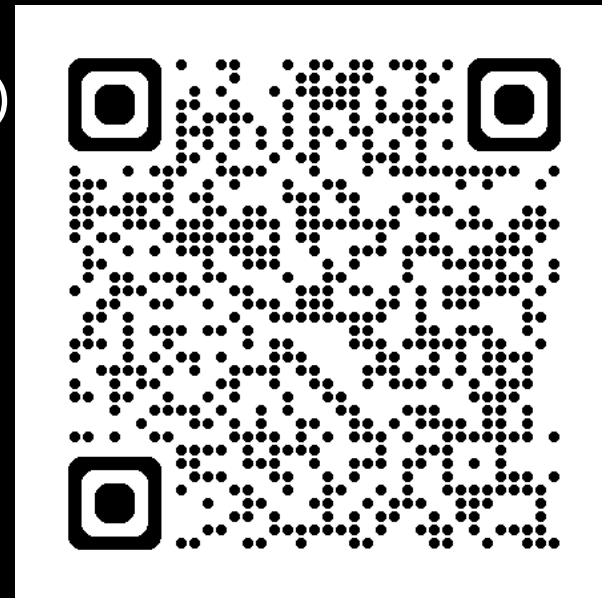


Next Community Call will 7th May 2025



Back to an US friendly time slot for this occurrence and then the one after will be back to this time slot 👍

Stay tuned to [issue #1901](#) (ALZ/ESLZ Repo)



Recordings will be available at:
aka.ms/ALZ/Community



This month's presenters:



Thank You!



Stay up-to-date:
aka.ms/ALZ/WhatsNew

