

This month's presenters:



Azure Landing Zones

7th May 2025 - External Community Call



Registration:

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

Agenda (please add suggestions):

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

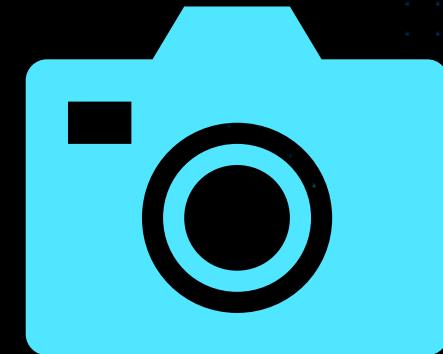
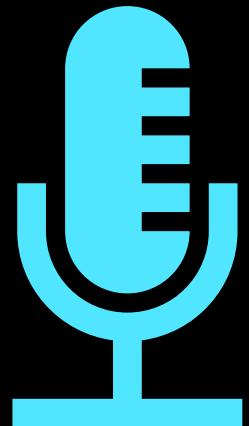
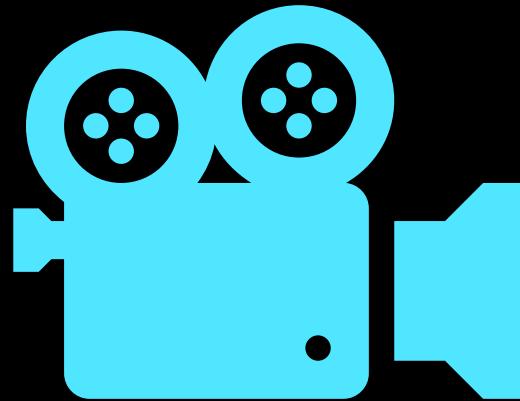




When you join this event, your name, email address and/or phone number may be viewable by other session participants in the attendee list. By joining, you're agreeing to this experience.



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

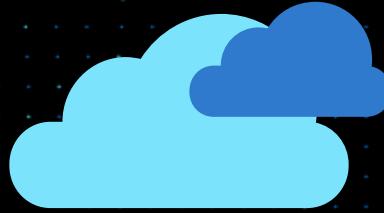


You can also opt out, if registered, by heading to:
aka.ms/alz/notifications/optout

Azure Landing Zones -
Notifications - Sign Up



Before we get started...

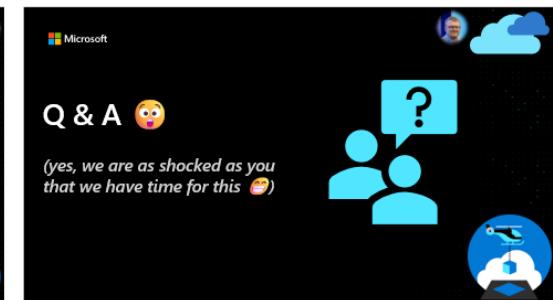
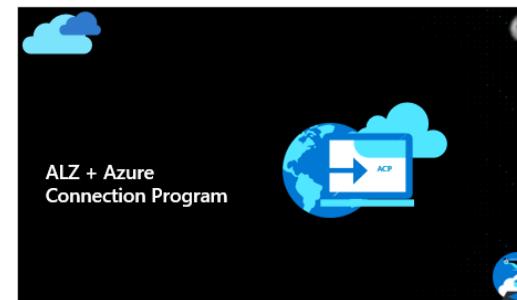
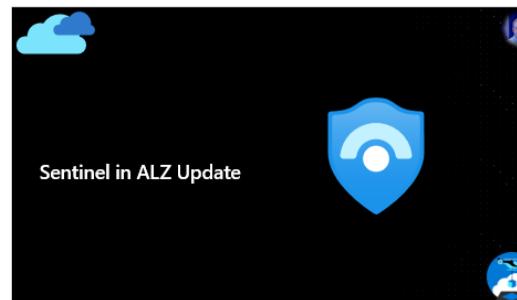
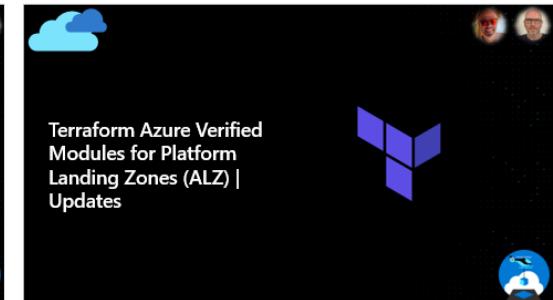
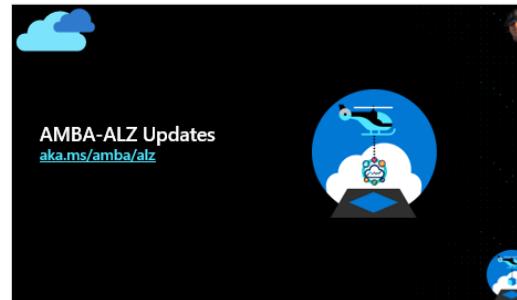
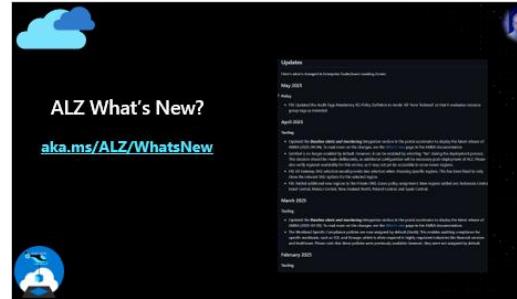
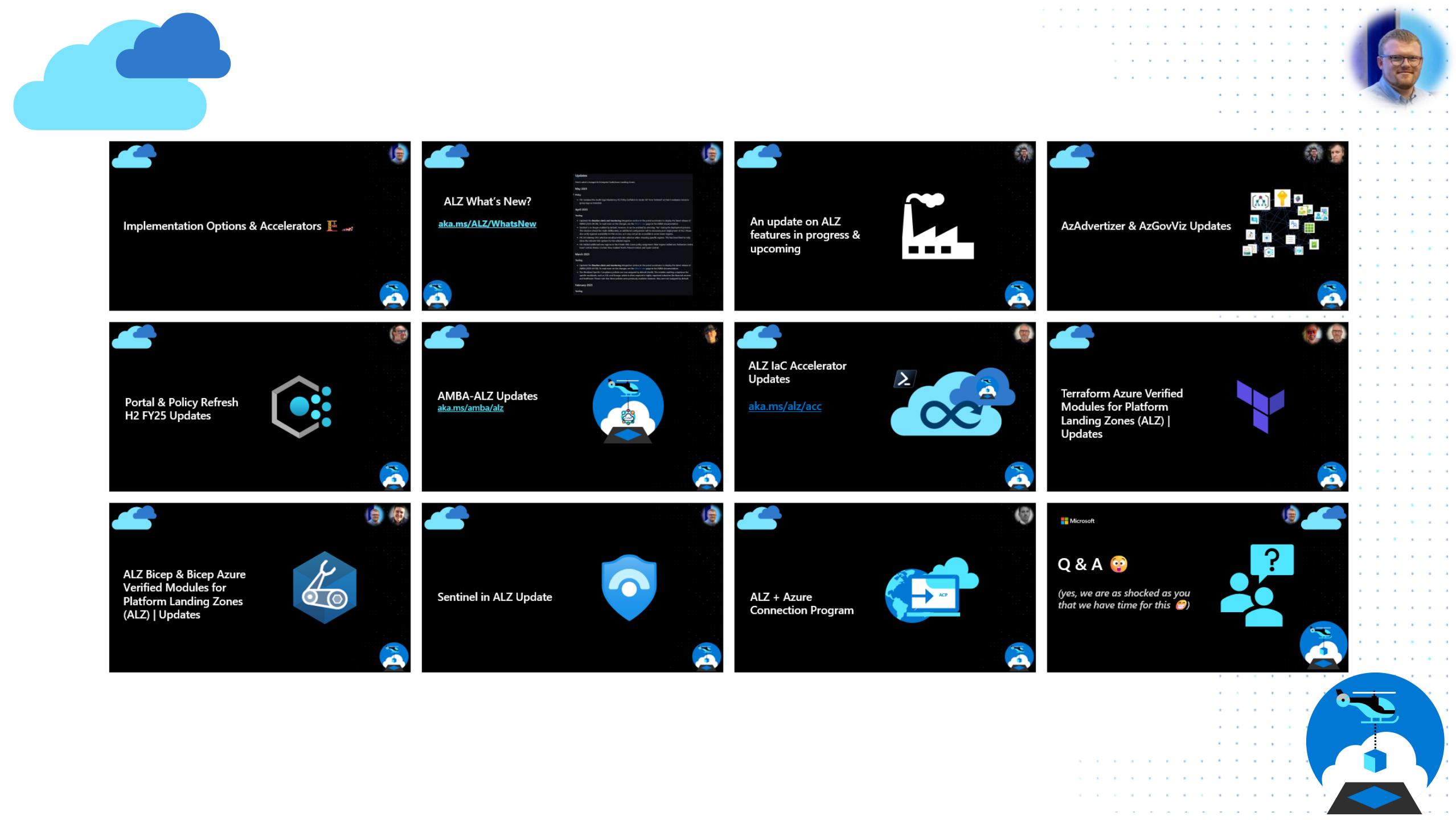


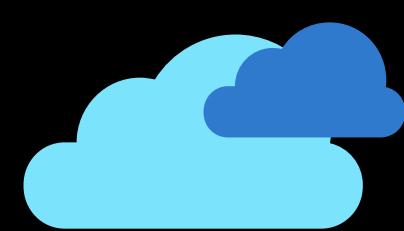
At any point, if you have a question please put it
in the chat!

(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 😊

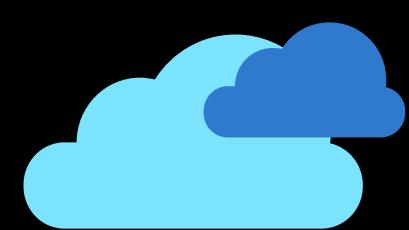






Implementation Options & Accelerators





Accelerators



Azure Architecture Center

[Browse all Architectures](#)

[Architecture icons](#)

[What's new](#)

▼ [Landing zones](#)

[Deployment options](#)

Subscription vending

After the platform landing zone and governance strategy is in place, the next step is to establish consistency about how subscriptions are created and operationalized 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 that platform teams use for workload teams to request subscriptions and platform teams to deploy and govern those subscriptions. It allows application teams to access Azure in a consistent and governed way, which helps ensure that requirements gathering is complete.

Organizations often have various styles of subscriptions that can be vended into their tenant, commonly referred to as [product lines](#). For more information, see [Establish common subscription vending product lines](#).

To get started, follow the [subscription vending implementation guidance](#). Then review the following IaC modules, which provide flexibility to fit your implementation needs.

[Expand table](#)

Deployment option	Description
Bicep subscription vending ¹	The subscription vending Bicep modules are designed to orchestrate the deployment of the individual application landing zones based on the configuration of each workload. They can be performed manually or as part of the automation process.
Terraform subscription vending ²	Modules use Terraform to orchestrate the deployment of the individual application landing zones.

Choose a platform landing zone approach

The following platform deployment options provide an opinionated approach to deploy and operate the [Azure landing zone conceptual architecture](#) as described in the Cloud Adoption Framework for Azure. The resulting architecture can vary based on the customizations, so it might not be the same for all the deployment options listed in this article. The differences between the platform deployment options are based on their use of different technologies, approaches, and customizations.

Standard deployment options

Standard deployment options address typical enterprise Azure usage.

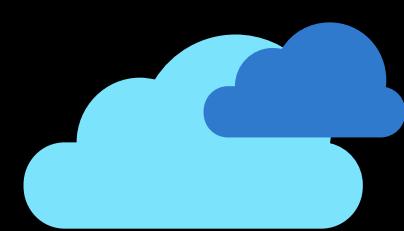
[Expand table](#)

Azure platform landing zone deployment option	Description
The Azure portal deployment	The Azure portal-based deployment provides a full implementation of the Azure landing zone conceptual architecture and opinionated configurations for key components, such as management groups and policies.
Bicep deployment	A modular deployment that's based on infrastructure as code (IaC), where each Bicep module encapsulates a core capability of the Azure landing zone conceptual architecture . These modules can be deployed individually, but the design recommends that you use orchestrator modules to encapsulate the complexity of deploying different topologies with the modules. Bicep deployment supports the Azure public cloud, Azure operated by 21Vianet regions, and Azure Infrastructure Services for US Government Clouds.
Terraform deployment ³	An IaC-based deployment that uses Azure-verified modules for platform landing zones and provides a customizable way to deploy Azure landing zones with Terraform.

Application landing zone architecture	Description
Azure App Service environment	Proven recommendations and considerations across both multitenant and App Service environment use cases with a reference implementation.
Azure API Management	Proven recommendations and considerations for how to deploy an internal API Management instance as part of a reference implementation. The scenario uses Azure Application Gateway to help provide secure ingress control and uses Azure Functions as the back end.
Azure Arc for hybrid and multicloud scenarios	Guidance for servers, Kubernetes, and Azure SQL Managed Instance enabled by Azure Arc.
Azure Container Apps	Guidance that outlines the strategic design path and defines the target technical state for deploying Container Apps. A dedicated workload team owns and operates this platform.
Azure Data Factory	Guidance about how to host a medallion lakehouse within an application landing zone.
Azure OpenAI Service chat workload	Guidance about how to integrate a typical Azure OpenAI chat application within Azure landing zones to use centralized shared resources while adhering to governance and cost efficiency. It provides guidance for workload teams about deployment and management.
AKS	Guidance and related IaC templates that represent the strategic design path and target technical state for an AKS deployment that runs within an application landing zone.
Azure Red Hat OpenShift	An open-source collection of Terraform templates that represent an optimal Azure Red Hat OpenShift deployment that includes Azure and Red Hat resources.
Azure Synapse Analytics	An architectural approach to prepare application landing zones for a typical enterprise deployment of Azure Synapse Analytics.
Azure Virtual Desktop	Azure Resource Manager (ARM), Bicep, and Terraform templates that you should reference when you design Azure Virtual Desktop deployments, which includes the creation of host pools, networking, storage, monitoring, and add-ons.
Azure Virtual Machines	An architecture that extends the guidance from the Virtual Machines baseline architecture to an application landing zone. It provides guidance about subscription setup, patch compliance, and other organizational governance concerns.
Azure VMware Solution	ARM, Bicep, and Terraform templates that you can use to help design Azure VMware Solution deployments. These deployments include Azure VMware Solution private cloud, jump box, networking, monitoring, and add-ons.
Citrix on Azure	Design guidelines for the Cloud Adoption Framework for Citrix Cloud in an Azure enterprise-scale landing zone that includes many design areas.
Red Hat Enterprise Linux (RHEL) on Azure	An open-source collection of architectural guidance and reference implementation recommendations that you can use to design RHEL-based workloads on Microsoft Azure.
High performance compute (HPC) workloads	An end-to-end HPC cluster solution in Azure that uses tools like Terraform, Ansible, and Packer. It addresses Azure landing zone best practices, which includes identity implementation, jump box access, and autoscaling.
Mission-critical workloads	Addresses how to design a mission-critical workload to run within an application landing zone.
SAP workloads	Provides guidance and recommendations for SAP workloads aligned to Azure landing zone best practices. Provides recommendations for how to create infrastructure components like compute, networking, storage, monitoring, and the build of SAP systems.



aka.ms/ALZ/AAC



ALZ What's New?

aka.ms/ALZ/WhatsNew



Updates

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

May 2025

Policy

- FIX: Updated the Audit-Tags-Mandatory-RG Policy Definition to mode 'All' from 'Indexed' so that it evaluates resource group tags as intended.

April 2025

Tooling

- Updated the *Baseline alerts and monitoring* integration section in the portal accelerator to deploy the latest release of AMBA (2025-04-04). To read more on the changes, see the [What's new](#) page in the AMBA documentation.
- Sentinel is no longer enabled by default. However, it can be enabled by selecting "Yes" during the deployment process. This decision should be made deliberately, as additional configuration will be necessary post-deployment of ALZ. Please also verify regional availability for this service, as it may not yet be accessible in some newer regions.
- FIX: ER Gateway SKU selection would provide two selectors when choosing specific regions. This has been fixed to only show the relevant SKU options for the selected region.
- FIX: Added additional new regions to the Private DNS Zones policy assignment. New regions added are: Indonesia Central, Israel Central, Mexico Central, New Zealand North, Poland Central, and Spain Central.

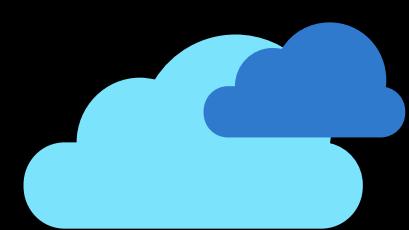
March 2025

Tooling

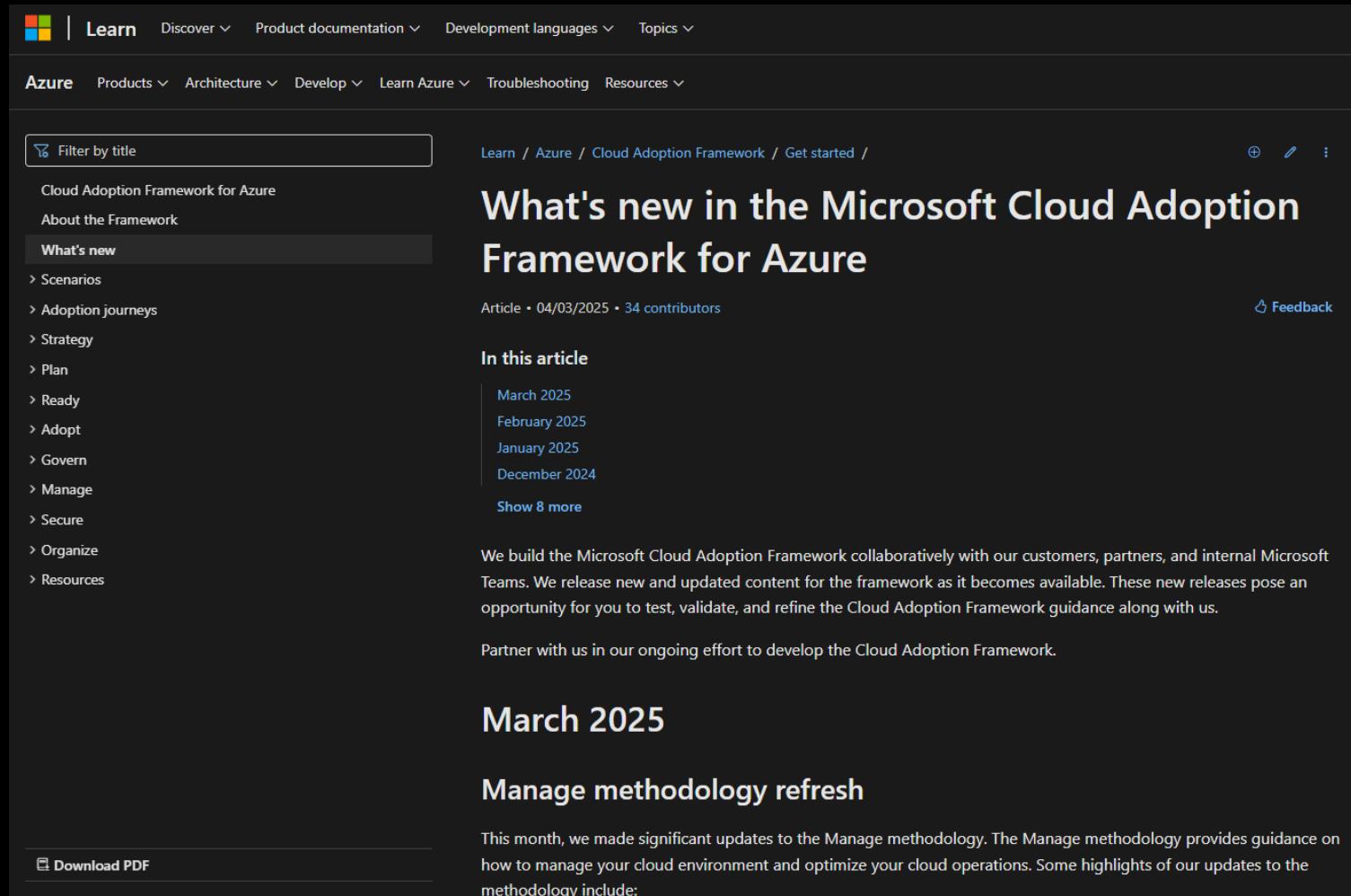
- Updated the *Baseline alerts and monitoring* integration section in the portal accelerator to deploy the latest release of AMBA (2025-03-03). To read more on the changes, see the [What's new](#) page in the AMBA documentation.
- The Workload Specific Compliance policies are now assigned by default (Audit). This enables auditing compliance for specific workloads, such as SQL and Storage, which is often required in highly regulated industries like financial services and healthcare. Please note that these policies were previously available; however, they were not assigned by default.

February 2025

Tooling



CAF What's New?



The screenshot shows a Microsoft Learn page for the Cloud Adoption Framework (CAF) in Azure. The main title is "What's new in the Microsoft Cloud Adoption Framework for Azure". The page is dated 04/03/2025 and has 34 contributors. It features a sidebar with navigation links like "Cloud Adoption Framework for Azure", "About the Framework", and "What's new" (which is currently selected). The "What's new" section lists various adoption journeys and methodologies. A "Show 8 more" link is present. The page also includes a "Feedback" button and a "In this article" sidebar with links to March 2025, February 2025, January 2025, and December 2024. A summary text states that the framework is built collaboratively and updated regularly. A "March 2025" section highlights a "Manage methodology refresh". A "Download PDF" button is at the bottom.

Learn | **Learn** Discover ▾ Product documentation ▾ Development languages ▾ Topics ▾

Azure Products ▾ Architecture ▾ Develop ▾ Learn Azure ▾ Troubleshooting Resources ▾

Filter by title

Learn / Azure / Cloud Adoption Framework / Get started /

What's new in the Microsoft Cloud Adoption Framework for Azure

Article • 04/03/2025 • 34 contributors [Feedback](#)

In this article

- March 2025
- February 2025
- January 2025
- December 2024

Show 8 more

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.

Partner with us in our ongoing effort to develop the Cloud Adoption Framework.

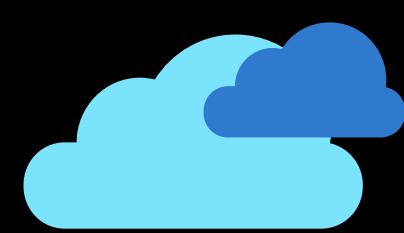
March 2025

Manage methodology refresh

This month, we made significant updates to the Manage methodology. The Manage methodology provides guidance on how to manage your cloud environment and optimize your cloud operations. Some highlights of our updates to the methodology include:

[Download PDF](#)





ALZ Public Roadmap

[aka.ms/ALZ/
Roadmap](https://aka.ms/ALZ/)

Azure / Projects / Azure Landing Zones Public Roadmap

Backlog | By priority | By size | New view

Filter by keyword or by field

⊕ We are thinking about... 1

- Draft
DNSSEC
Low Small

⊕ What we are working on... 18

- Draft
Sentinel future in ALZ
Medium X-Large
- Draft
DDoS IP Protection Support
Low Medium
- Draft
DNS security policy
Low Small
- Draft
Terraform Azure Verified Modules for Platform Landing Zones (ALZ) Migration Guidance & Tooling
High Large
- Draft
Fallback to Internet for Private DNS Zone
Low Small
- Draft
Azure Firewall - New Management NIC
Medium Large

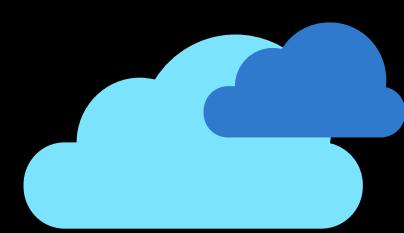
⊕ What we have completed 22

- Draft
Zone redundancy enhancements
High Medium
- Draft
Retirement of NSG flow logs
High Large
- Draft
Azure Policy Versioning ALZ strategy
High Medium
- Draft
Bicep automation in the ALZ Accelerator
High X-Large
- Draft
Subscription vending guidance for common application landing zone vending scenario's
Medium Medium
- Draft
ALZ Portal and AVNM
Medium Large

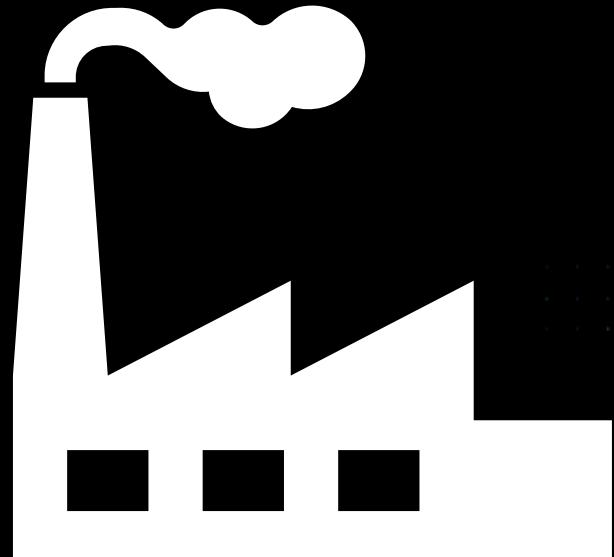
⊕ What we have parked... 3

- Draft
'Enterprise-Scale' rename to 'Azure Landing Zones' (repos)
Low X-Large
- Draft
Log analytics design refresh for ALZ
Medium X-Large
- Draft
Removing non-Availability Zones SKUs for Virtual network gateways from all accelerators
High Medium





An update on ALZ
features in progress &
upcoming





ALZ features alignment progress

✓ What we have completed

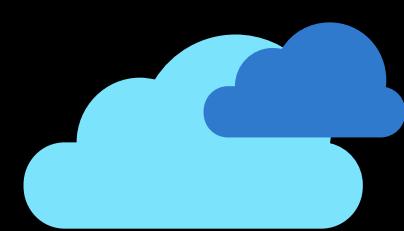
- Deprecation of NSG flow logs in-favor of Virtual network flow logs
- Deployment of Sidecar network for vWan topology (Terraform and coming very soon to the Portal)
- Azure Bastion (Coming very soon to the Portal)
- Azure Firewall management subnet (docs are updated and coming very soon to the Portal)

⌚ What we are working on

- Private DNS resolver (Bicep and Portal)
- Refreshing private DNS architecture for ALZ
- Deprecation of default outbound internet access
- Azure Virtual Network Manager
- Deprecation of non-AZ Virtual network gateways

📋 We are thinking about

- Network Security Perimeter
- Public DNS zones (DNSSEC, DNS security policies)
- New vWan features (route-maps)
- New Azure Firewall features (draft firewall policies, BYOIP support for secured virtual hubs, ...etc)
- Private DNS fallback to the internet



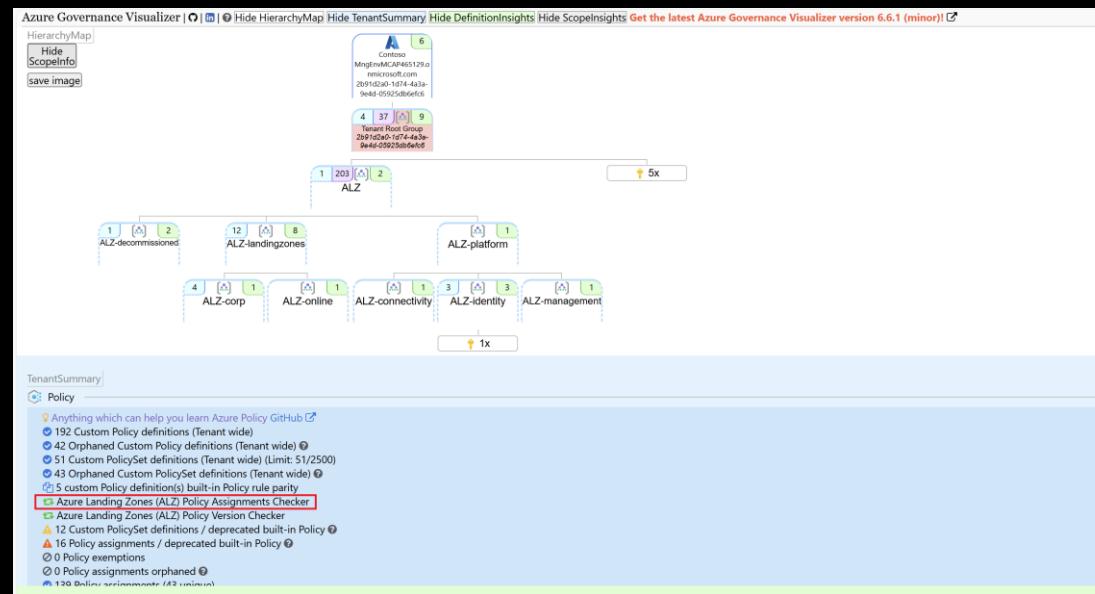
AzAdvertiser & AzGovViz Updates



AzGovViz ALZ Policy Assignments Checker



How to keep up with ALZ policy releases ?



Azure Landing Zones (ALZ) Policy Assignments Checker					
Rows: 44			?		
Clear	ALZ Management Group	Management Group exists / provided	Missing ALZ Policy Assignments	Clear	ALZ release
	sandboxes	✓ x	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

7e8db15 · Azure-Landing-Zones-Library / platform / alz / policy_assignments / Enable-DDoS-VNET.alz_policy.assignment.json

3 people · feat: update platform/alz library (automated) (#76) · Go to file · efd6d56 · last month · History

Code Blame 26 lines (26 loc) · 1.82 kB

```
1  {
2     "type": "Microsoft.Authorization/policyAssignments",
3     "apiVersion": "2022-06-01",
4     "name": "Enable-DDoS-VNET",
5     "location": "Global",
6     "dependsOn": [],
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        "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/9d62e2d0-ebc1-4caf-ad78-5d4f7bcb83d3d",
14        "enforcementMode": "Default",
15        "parameters": {
16            "ddosPlan": {
17                "value": "subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/placeHolder/providers/Microsoft.Network/ddosProtectionPlans/placeHolder"
18            }
19        },
20        "effect": {
21            "value": "Modify"
22        }
23    },
24    "scope": "/providers/Microsoft.Management/managementGroups/placeHolder",
25    "metaScopes": []
26 }
```

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

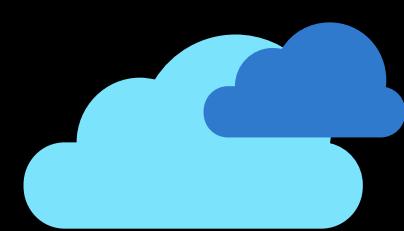
AzPolicyAdvertiser

⌚ last sync: 2024-Nov-11 18:54:29 UTC

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	94d42ad3-ecb1-4caf-ad78-5d47bcb83d3d														
Version	1.8.1														
	Details on versioning ⓘ														
Versioning	Versions supported for Versioning: 2 1.8.0 1.8.1 Built-in Versioning [Preview] ⓘ														
Category	Network Microsoft Learn ⓘ														
Description	Protect your virtual networks against volumetric and protocol attacks with Azure DDoS 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)	<table border="1"><tr><th>Role Name</th><th>Role Id</th></tr><tr><td>Network Contributor</td><td>4d97098b-3d4f-4787-a291-c67834d21127</td></tr></table>	Role Name	Role Id	Network Contributor	4d97098b-3d4f-4787-a291-c67834d21127										
Role Name	Role Id														
Network Contributor	4d97098b-3d4f-4787-a291-c67834d21127														
Role aliases	IF (2) <table border="1"><tr><th>Alias</th><th>Namespace</th><th>ResourceType</th><th>Path</th><th>PathsDefault</th><th>DefaultPath</th><th>Modifiable</th></tr><tr><td>Microsoft.Network/virtualNets</td><td>Microsoft.Network</td><td>virtualNetworks</td><td>properties.ddosProtection</td><td>True</td><td></td><td>True</td></tr></table>	Alias	Namespace	ResourceType	Path	PathsDefault	DefaultPath	Modifiable	Microsoft.Network/virtualNets	Microsoft.Network	virtualNetworks	properties.ddosProtection	True		True
Alias	Namespace	ResourceType	Path	PathsDefault	DefaultPath	Modifiable									
Microsoft.Network/virtualNets	Microsoft.Network	virtualNetworks	properties.ddosProtection	True		True									



New Feature: AzResourceTypesAdvertiser



HOME POLICY INITIATIVE ALIAS COMPLIANCE **RESOURCETYPES** AZURE ACCESS CONTROL ENTRA-ID ACCESS CONTROL CATCHUP ⓘ

last sync: 2025-May-05 19:52:12 Etc/UTC

Clear all filters ⓘ

RT [Resource type] base RP [Resource Provider] details

Resource type ▾	RP Aliases and Azure Policy										RP RBAC Operations and Roles & Roles related operation actions			
	Resource Provider	Resource Provider displayName	#Resource types	#Resource Provider aliases	Resource Provider aliases	Resource Provider Azure Policy	#Resource Provider operations	Resource Provider operations	Resource Provider RBAC roles	Related 1st party Service Principal(s)				
compute/virtualmachines Snapshot	Microsoft.Compute	Microsoft Compute	132	2161	Resource Provider aliases	then.operations:0 487 Policy definitions if:480 then.deployment:182 then.details:2 then.existenceCondition:0 then.operations:0	279	Resource Provider operations	64 unique RBAC roles action:34 delete:22 read:59 write:30	count:9 • Azure Compute appId:579d9c9d-4cf4-8124-7eba65ed3356 • Azure Regional Service Manager appId:5e5e43d4-54da-4211-86a4-c6e7f3 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e00				
microsoft.compute/virtualmachines/extensions Snapshot	Microsoft.Compute	Microsoft Compute	132	2161	Resource Provider aliases	487 Policy definitions if:480 then.deployment:182 then.details:2 then.existenceCondition:0 then.operations:0	279	Resource Provider operations	64 unique RBAC roles action:34 delete:22 read:59 write:30	count:9 • Azure Compute appId:579d9c9d-4cf4-8124-7eba65ed3356 • Azure Regional Service Manager appId:5e5e43d4-54da-4211-86a4-c6e7f3 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e00				
microsoft.compute/virtualmachines/instanceview Snapshot	Microsoft.Compute	Microsoft Compute	132	2161	Resource Provider aliases	487 Policy definitions if:480 then.deployment:182 then.details:2 then.existenceCondition:0 then.operations:0	279	Resource Provider operations	64 unique RBAC roles action:34 delete:22 read:59 write:30	count:9 • Azure Compute appId:579d9c9d-4cf4-8124-7eba65ed3356 • Azure Regional Service Manager appId:5e5e43d4-54da-4211-86a4-c6e7f3 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e00				
microsoft.compute/virtualmachines/metricdefinitions Snapshot	Microsoft.Compute	Microsoft Compute	132	2161	Resource Provider aliases	487 Policy definitions if:480 then.deployment:182 then.details:2 then.existenceCondition:0 then.operations:0	279	Resource Provider operations	64 unique RBAC roles action:34 delete:22 read:59 write:30	count:9 • Azure Compute appId:579d9c9d-4cf4-8124-7eba65ed3356 • Azure Regional Service Manager appId:5e5e43d4-54da-4211-86a4-c6e7f3 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e00				



New Feature: AzResourceTypesAdvertiser

AzResourceTypeAdvertiser

last sync: 2025-May-05 19:52:12 Etc/UTC

Virtual Machines - Microsoft Azure Resource type
microsoft.compute/virtualmachines

Resource provider (RP) - Microsoft Compute [Microsoft.Compute]

RP Microsoft.Compute

RP display name Microsoft Compute

RP Resource types

RP aliases

RP Azure Policy

Azure Policy definitions: 487

* if: 480

* then.deployment: 182

* then.details: 2

* then.existenceCondition: 0

* then.operations: 0

RP RBAC operations

RP RBAC operations: 279

* RP RBAC operationType action: 94

* RP RBAC operationType delete: 37

* RP RBAC operationType read: 106

* RP RBAC operationType write: 42

RP RBAC Roles & Operation actions

Unique RBAC Roles: 64

* RBAC Roles with action operationType: 34

* RBAC Roles with delete operationType: 22

* RBAC Roles with read operationType: 59

* RBAC Roles with write operationType: 30

RP related 1st party Service Principals

RP related 1st party Service Principals: 9

* Microsoft Azure Windows Virtual Machine Sign-in (Azure Windows VM Sign-In) (appId: 372140e0-b3b7-4226-8ef9-d57986796281) [JSON;CSV]

* Microsoft Azure Linux Virtual Machine Sign-in (Azure Linux VM Sign-In) (appId: cebff148-7fc-4685-bb0e-f6afdfcf8ed) [JSON;CSV]

* Marketplace Catalog API (appId: 18009ca-4369-477-5580ee5eb08d) [JSON;CSV]

* Compute User Provider (appId: a903894e-f1d0-4e37-bf10-67a54a0596) [JSON;CSV]

* Compute Resource Provider (Managed Disk Resource Provider) (appId: 606cd5d7-0c8c-4951-993c-23c25a2169af) [JSON;CSV]

* Compute Recommendation Service (appId: b9a92e36-2cf8-4f4a-bcb3-9d99e0e014ab) [JSON;CSV]

* Compute Artifacts Publishing Service (appId: a8b6fb88-1d1a-4626-b040-9a729ea93c65) [JSON;CSV]

* Azure Regional Service Manager (appId: 5e5e43d4-54da-4211-86a4-c6e7f3715801) [JSON;CSV]

* Azure Compute (appId: 579d9c9d-4c83-4afe-8124-7eba65ed3356) [JSON;CSV]

All Azure RPs

* Microsoft Learn

* AzResourceTypesAdvertiser (Microsoft only)

Resource type (RT) - Virtual Machines [microsoft.compute/virtualmachines]

RT information

RT microsoft.compute/virtualmachines

RT display name Virtual Machines

RT type only (without RP) virtualMachines

RT sub-Resource types sub-Resource types: 13

RT schema

RT schema API versions: 26

- 2024-11-01
- 2024-07-01
- 2024-03-01
- 2023-10-01
- 2023-07-01
- 2023-03-01
- 2022-11-01
- 2022-08-01
- 2022-03-01

All Microsoft Azure RTs

Assessment tooling

Azure Advisor

Azure Advisor recommendations: 80

- Cost [High] Reduce size of shutdown underutilized virtual machines
- Cost [Medium] Migrate VMs to a lower cost VM size
- HighAvailability [High] Migrate workload to D-series or better virtual machine
- HighAvailability [High] Standard_NC2v3 virtual machine (VM) size in NCv3-series is being retired.
- HighAvailability [High] Update your outbound connectivity protocol to Service Tags for Azure Site Recovery
- HighAvailability [High] Upgrade to a newer offer of a virtual machine image
- HighAvailability [High] Upgrade to a newer SKU for Virtual Machine Image
- HighAvailability [High] Upgrade your deprecated Virtual Machine image to a newer image

Azure Proactive Resilience Library v2

Azure Proactive Resilience Library v2 recommendations: 18

- DisasterRecovery [High] Validate VM functionality with a Site Recovery test failover to check performance at target
- DisasterRecovery [Medium] Replicate VMs using Azure Site Recovery
- DisasterRecovery [Medium] Reserve Compute Capacity in Disaster Recovery Regions
- DisasterRecovery [Medium] Backup VMs with Azure Backup service
- HighAvailability [High] Reserve Compute Capacity for critical workloads
- HighAvailability [High] Use maintenance configurations for the VMs
- HighAvailability [High] Run production workloads on two or more VMs using VMSS Flex
- HighAvailability [High] Use Managed Disks for VM disks

PSRule for Azure

PSRule for Azure recommendations: 19

- Cost Optimization [Awareness] Multi-Region Hosting Rights
- Cost Optimization [Awareness] Use current VM SKU
- Cost Optimization [Awareness] Use current VM SKU
- Operational Excellence [Awareness] Use valid VM computer names
- Operational Excellence [Awareness] Use valid VM names
- Operational Excellence [Awareness] Upgrade to Azure Monitor Agent
- Operational Excellence [Important] Use Azure Monitor Agent
- Operational Excellence [Important] Virtual Machine agent is not provisioned

Azure Quick Review (AQR)

Azure Quick Review (AQR) recommendations: 25

- DisasterRecovery [Medium] Backup VMs with Azure Backup service
- DisasterRecovery [Medium] Replicate VMs using Azure Site Recovery
- Governance [Low] Ensure that your VMs are compliant with Azure Policies
- Governance [Low] Review VMs that are stopped
- Governance [Low] Ensure VM names still comply with naming conventions
- Governance [Low] Virtual Machine should have tags
- HighAvailability [High] Deploy VMs across Availability Zones
- HighAvailability [High] Reserve Compute Capacity for critical workloads

Infrastructure as Code (IaC)

ARM (Azure Resource Manager) template API versions: 26

- latest
- 2024-07-01
- 2024-03-01
- 2023-09-01
- 2023-07-01
- 2023-01-01
- 2022-11-01
- 2022-08-01
- 2022-03-01

Bicep templates

Bicep template API versions: 26

- latest
- 2024-11-01
- 2024-07-01
- 2024-03-01
- 2023-09-01
- 2023-07-01
- 2023-03-01
- 2022-11-01
- 2022-08-01
- 2022-03-01

Terraform providers

Terraform provider: 6

- linux_virtual_machine

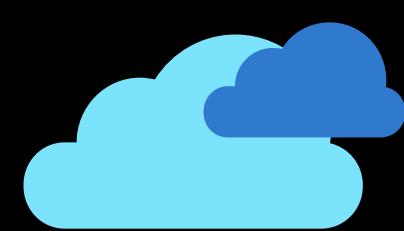
Azure Verified Modules (AVM) Bicep

Azure Verified Modules (AVM) Terraform

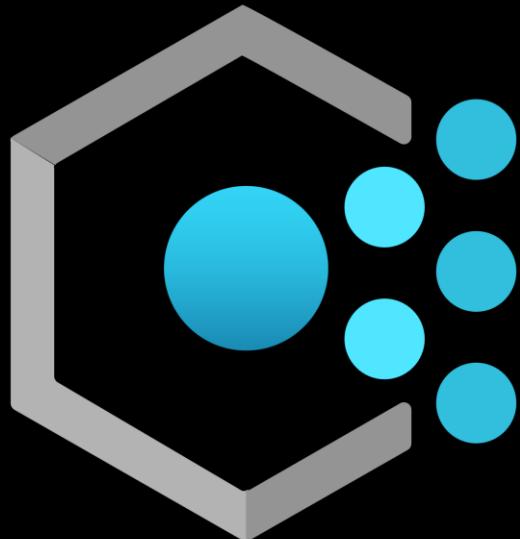
VIRTUAL MACHINE

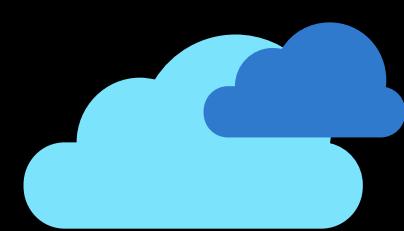
- GitHub: [Virtual Machine](#)
- Terraform registry: [Virtual Machine](#)





Portal & Policy Refresh H2 FY25 Updates





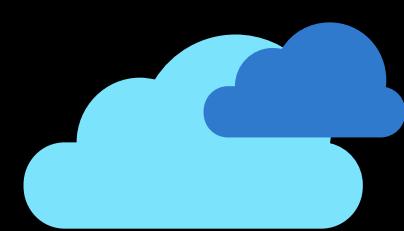
ALZ Policy News

aka.ms/alz/whatsnew



- Policy Refresh H2 FY25 (June 2025)
 - Delayed for portal updates
 - Always review "What's New"
 - One "breaking" change – initiative cleanup
 - Cleanup and update of the Excel
- New
 - Added support for Defender for AI workloads
 - Added initiative for Guest Attestation for Trusted Launch VMs
- Policy Versioning
 - Only works for portal
 - TF/Bicep coming soon
- General fixes
 - Remove/replace all deprecated policies
- Community requests
 - MDFC expose all available parameters (incl. Server plans :))
 - Updated DomainJoin policy to support newer versions of Windows





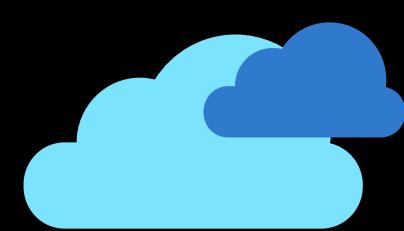
ALZ Portal News

aka.ms/alz/portal



- Networking
 - Add support for Azure Bastion for all network topologies
 - Add support for Azure Private DNS Resolver for all network topologies (needs last mile config)
 - Added VWAN provisioning of sidecar network (needed for Bastion & Private DNS)
 - All Firewall SKUs now deploy with management NIC in the AzureFirewallManagementSubnet
- Workload Specific Compliance
 - Updated descriptions and options for clarity
 - Changed to default to "Audit Only" for all initiatives at default scopes (Platform/Landing Zones)
- Remove support of non-public regions





AMBA-ALZ Updates

aka.ms/amba/alz





AMBA Updates

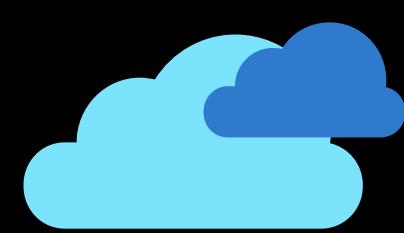
- New features and alerts:
 - Exclusion of MG and Subscriptions at scale during deployment
 - Securely store log-search alerts using CMK
 - Exclusion of logical disks for both Azure and Hybrid VM alerts
- New Web initiative alerts for:
 - *LA Workspace Daily Cap Limit Reached Alert*
 - *Activity Log LA Workspace Workspace Regenerate Key Alert*
 - *Activity Log LA Workspace Delete Alert*
- Optimization of Azure Resource Graph calls used inside log-search alerts

aka.ms/amba/alz/whatsnew

- **4** bugs fixed
- Documentation improvements
- Enforced naming convention for AMBA-ALZ policy definitions, policy initiatives and policy assignments

Name ↑	Latest version... ↑	Definition location ↑	Polic... ↑	Type ↑
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) - Notification Assets	1.0.0	BR1-Non-ALZ	2	Custom
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Web	1.0.0	BR1-Non-ALZ	9	Custom
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Azure Virtual Machines	1.0.0	BR1-Non-ALZ	11	Custom
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Storage	1.0.0	BR1-Non-ALZ	2	Custom
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Service Health	1.0.0	BR1-Non-ALZ	6	Custom
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Recovery Services	1.0.0	BR1-Non-ALZ	2	Custom
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Changes in Network Routing and Security	1.0.0	BR1-Non-ALZ	4	Custom



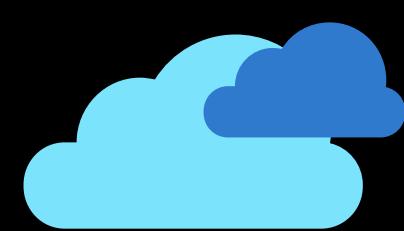


AMBA Roadmap

aka.ms/amba/roadmap/alz

- 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.
- Investigating Lighthouse support for ALZ pattern
 - Adding alerts for:
 - Azure Monitor Ingestion limit alert
 - Network Resources:
 - Microsoft.Network/azureFirewalls
 - Microsoft.Network/p2svpnGateways
 - Microsoft.Network/virtualhubs
 - Microsoft.Network/expressrouteGateways
 - Additional documentation for:
 - AMBA-ALZ alerts testing





AMBA Roadmap

aka.ms/amba/roadmap/alz



AMBA Public Roadmap

By Status | By priority | By effort | + New view

pattern:alz

Backlog (1) Estimate: 0

This item hasn't been started

Draft Deploy with Bicep

Medium X-Large ALZ

In Progress (5) Estimate: 0

This is actively being worked on

Draft Service Health policies transition to Built-in policies

Urgent X-Large ALZ

Draft Deploy with Terraform

Medium X-Large ALZ

Draft Documentation Update: How to test AMBA-ALZ alerts

Medium Medium ALZ

Draft Investigate Lighthouse support for AI-7 pattern

Completed (12) Estimate: 0

This has been completed

Draft Add alerts for Route and Route Table delete

Urgent Medium ALZ

Draft Arg query optimization

Urgent Large ALZ

Draft BUG: Resource group name customization in AMBA-ALZ Portal deployment is not honored

Urgent Medium ALZ

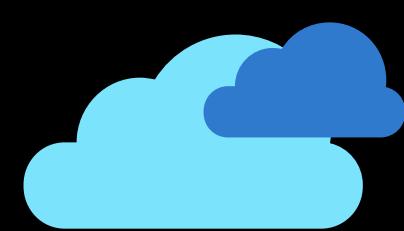
Draft BUG: Missing mandatory Platform MG mandatory param value

Parked (1) Estimate: 0

Azure Monitor Ingestion limit alert

Medium Medium ALZ





ALZ IaC Accelerator Updates

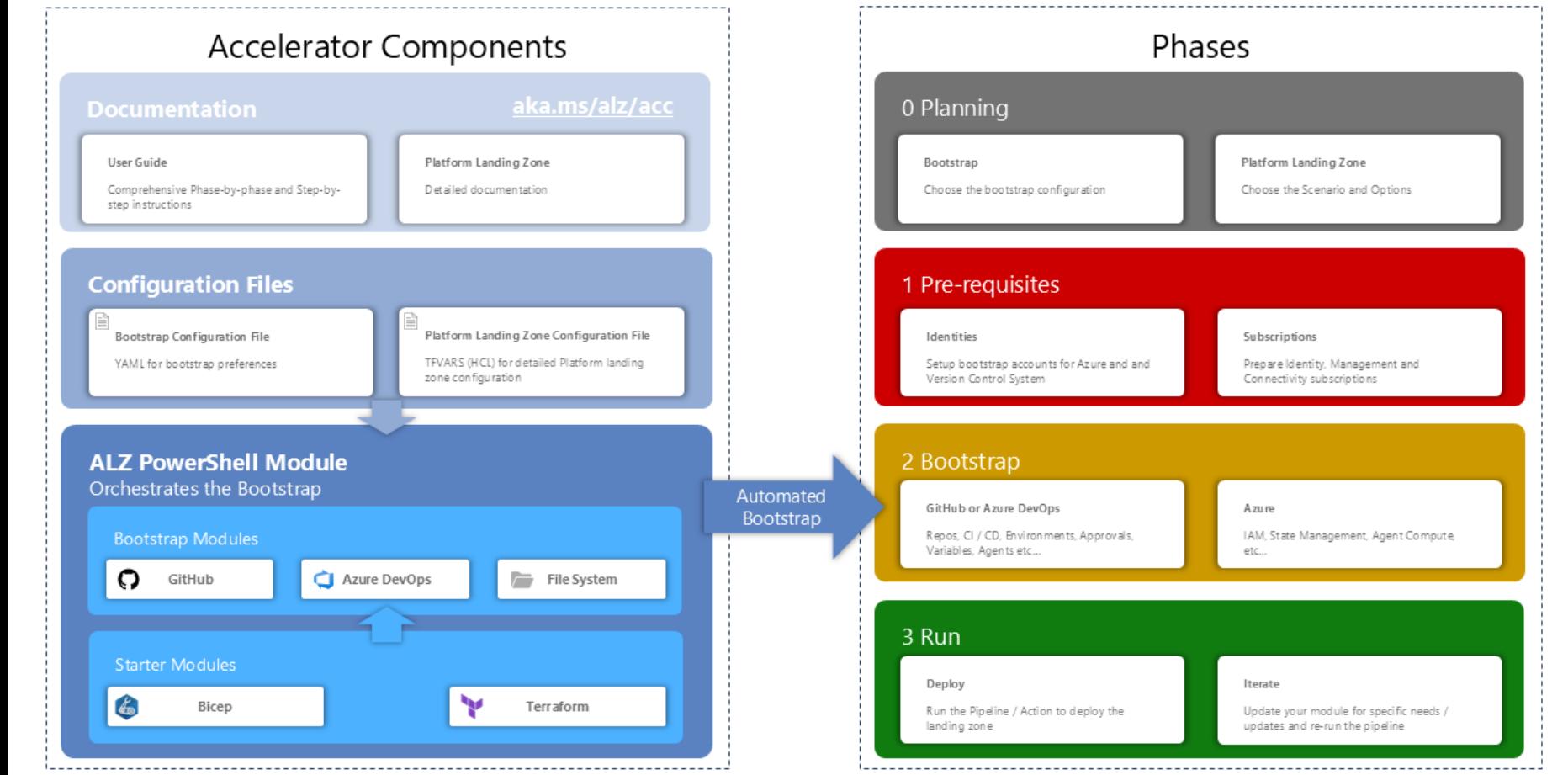
aka.ms/alz/acc



How the ALZ IaC Accelerator Works?



Azure Landing Zones IaC Accelerator



What's new with the Terraform ALZ IaC Accelerator?



- Simplified connectivity pattern modules
 - [avm-ptn-alz-connectivity-hub-and-spoke-vnet](#)
 - [avm-ptn-alz-connectivity-virtual-wan](#)
- Simpler upgrade path
 - [Upgrade guide](#)



What's coming to the ALZ IaC Accelerator?

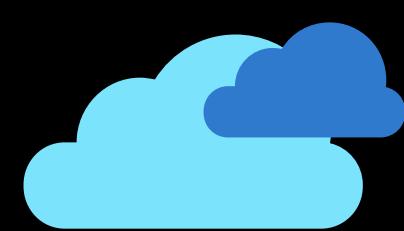
- Allow different connectivity configurations per hub for Terraform (this month)
- Bicep Azure Verified Modules for Platform Landing Zone (ALZ)
 - [Blog post](#) 
- Application landing zones
 - Subscription vending
 - Azure resources - network, peering, etc...
 - Bootstrapping for application teams with Azure DevOps and GitHub
 - First iteration this year



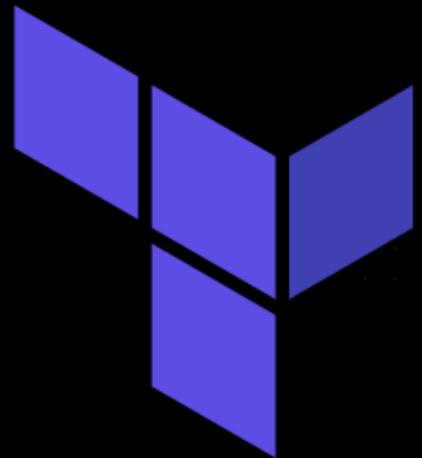
Sneaky plug...

- Azure DevOps ID Token Refresh and Terraform Task v5: [Blog Post](#) 

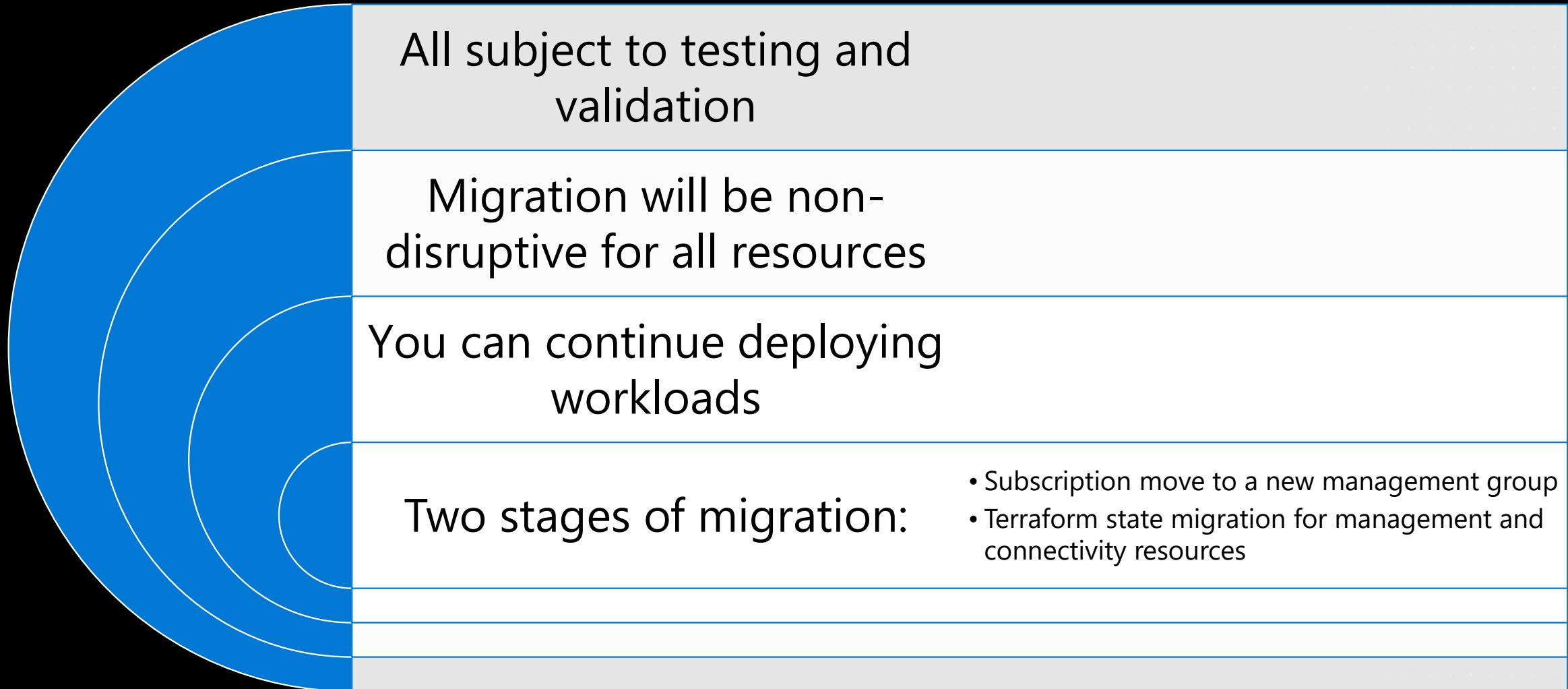




Terraform Azure Verified Modules for Platform Landing Zones (ALZ) | Updates



Proposed Migration Approach (reminder)

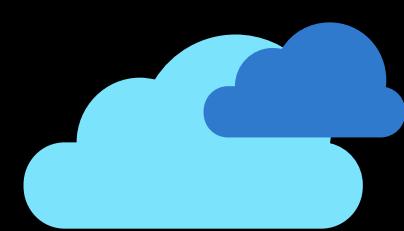


Support statement for caf-enterprise-scale

caf-enterprise-scale will be fully supported up until the release of the migration tooling

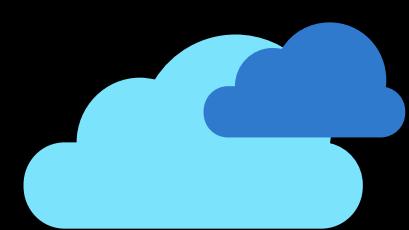
Once migration tooling released, we will provide an additional 1-year of extended support to caf-enterprise-scale for quality and policy updates (not features)

After this 1-year period, the repository will be archived - no further updates will be made



ALZ Bicep & Bicep Azure Verified Modules for Platform Landing Zones (ALZ) | Updates



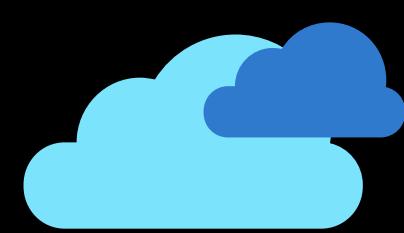


ALZ-Bicep | Updates



- Release of [v0.22.2](#) hot off the press!
 - Fixed some configuration issues with Azure Monitoring Agent related resources
- Some other updates from other releases as of the last community call:
 - New module for workload-specific policy assignments
 - Refactored ALZ Defaults policy assignments module
 - Added support for specifying virtual network gateway IP configuration names
 - Improved handling of null values in custom policy definitions
- See full release notes from all releases [here](#)!

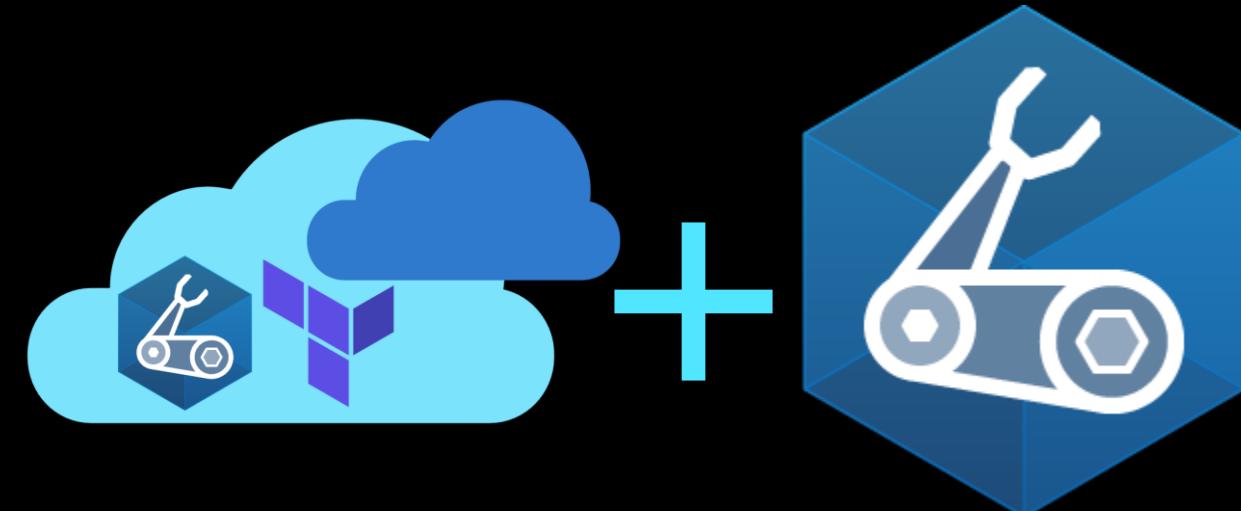




Bicep Azure Verified Modules for Platform Landing Zones (ALZ) | Update

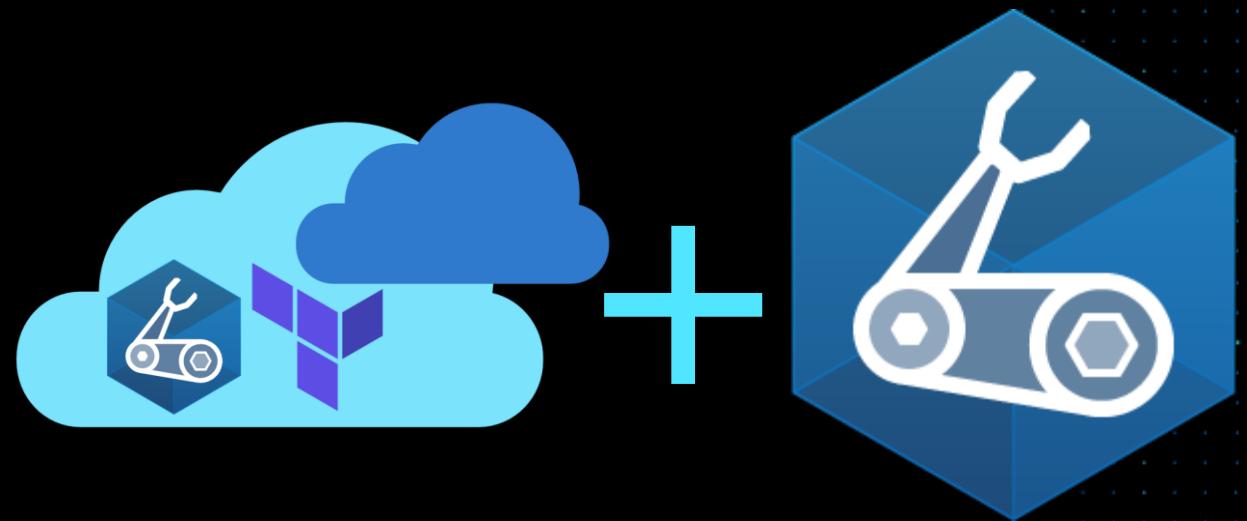


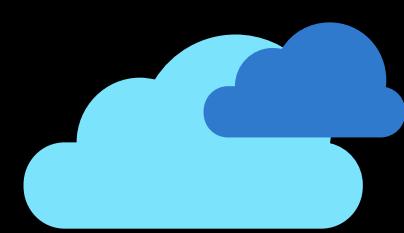
- See [An Update on Bicep Azure Verified Modules for Platform Landing Zone \(ALZ\) | Microsoft Community Hub](#)
- **Soft Launch Target:** June–July 2025
- Preview Available: ``avm/ptn/alz/empty``
- "Max" Test case for depth example
- Coming Soon (based on [feedback](#))
 - ``avm/ptn/alz/int-root``
 - ``avm/ptn/alz/platform``
 - ``avm/ptn/alz/platform-management``
 - ``avm/ptn/alz/platform-identity``
 - ``avm/ptn/alz/platform-connectivity``
 - ``avm/ptn/alz/landing-zones``
 - ``avm/ptn/alz/landing-zones-corp``
 - ``avm/ptn/alz/landing-zones-online``
 - ``avm/ptn/alz/decommissioned``
 - ``avm/ptn/alz/sandbox``





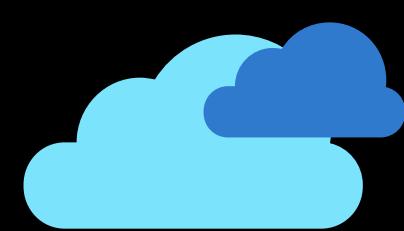
Demo





Sentinel in ALZ Update





Thanks for all your feedback on



github.com/Azure/Enterprise-Scale/discussions/1898



Azure / Enterprise-Scale

Code Issues 86 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) [Edit](#)

#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)
 - Often organizations have separate Security teams requesting/driving this
 - Product Group guidance leans to single workspace by default, see [here](#).
- Do we need a separate "Security" platform Subscription?
 - Can't 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?

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 & Audit... Needs: More Evidence... Status: Help Wanted... Type: Enhancement... Type: Feature Request...

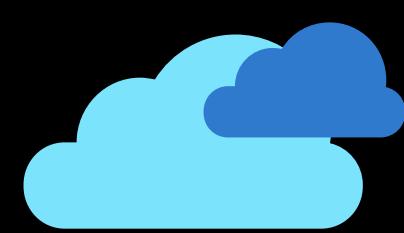
1 participant

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





We now have a proposal to implement

github.com/Azure/Enterprise-Scale/discussions/1978
[\(aka.ms/alz/sentinelfuture\)](https://aka.ms/alz/sentinelfuture)



What we propose going forward in ALZ in regards to Sentinel

1. A dedicated SIEM/Security subscription in the Management, Management Group
 - As per a number of the comments RBAC should be done at the Subscription scope and **not** the Management Group scope so therefore a dedicated Management Group for just Sentinel/Security/SIEM we don't feel is warranted or needed at this time. Plus it makes these proposed changes less "breaking" as the ALZ hierarchy and policy assignments don't need to change 
2. This subscription will not have anything deployed into it and will be **empty** due to:
 - We do not want to trigger the [Sentinel free trial](#) earlier than you are ready
 - A lot of customers, partners, ISVs etc. have their own ways of deploying and managing their Sentinel deployments and therefore we don't want to get in the way of that and make onboarding to these ways harder post ALZ deployment.
 - We can always build some AVM modules to help deploy and manage the LAW and Sentinel onboarding and management aspects, if requested... <https://aka.ms/avm/moduleproposal>



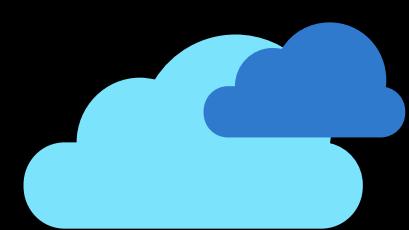
Some notes on the proposal above

1. We will expect the subscription to be created outside of ALZ, e.g. via [Subscription Vending](#) or manually, so that when you deploy ALZ it already exists
 - We will then just move it to the Management, Management Group
2. We will update the ALZ diagram and Visio with these changes
3. We will update any ALZ MS Learn CAF Documentation relating to these Sentinel decisions for ALZ



ALZ + Azure Connection Program





ALZ Influencers Group (Pilot)



- **Update**
 - **Nominations reviewed – thank you!**
 - **Azure Connections Program (ACP) is being migrated soon**
 - **Email will be sent following migration from ALZ team**
 - **Not taking further nominations at this stage**





Azure Landing Zones

17th September 2025 - External Community Call

Registration:

aka.ms/ALZ/CommunityCallRegister

Agenda (please add suggestions):

aka.ms/ALZ/CommunityCallAgenda

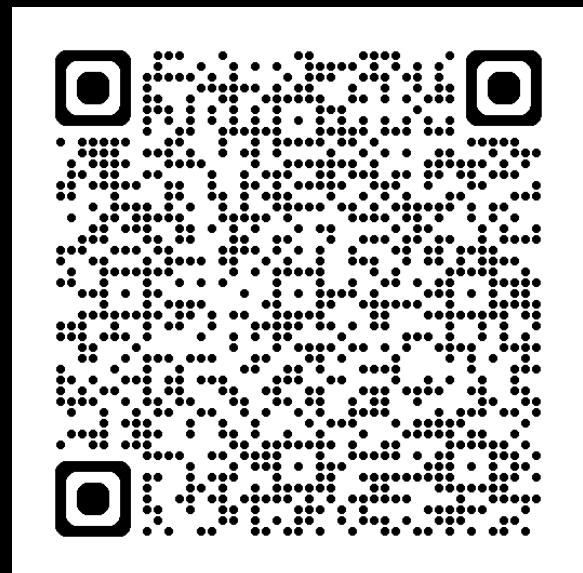




Next Community Call will 17th September 2025

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

Stay tuned to [issue #1987](#) (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

