

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>

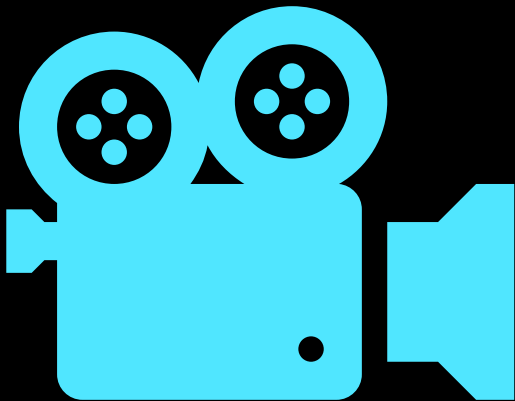




When you join this event, your name, email address and/or phone number may be viewable by other session participants in the attendee list. By joining, you're agreeing to this experience.



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

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 What's New?
aka.ms/ALZ/WhatsNew



An update on ALZ features in progress & upcoming




AzAdvertiser & AzGovViz Updates




Portal & Policy Refresh H2 FY25 Updates




AMBA-ALZ Updates
aka.ms/amba/alz



ALZ IaC Accelerator Updates
aka.ms/alz/acc




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




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





Sentinel in ALZ Update



ALZ + Azure Connection Program



Q & A 
(yes, we are as shocked as you that we have time for this 🤖)





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	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	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	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?



 | **Learn** [Discover](#) [Product documentation](#) [Development languages](#) [Topics](#)

Azure [Products](#) [Architecture](#) [Develop](#) [Learn Azure](#) [Troubleshooting](#) [Resources](#)

[Cloud Adoption Framework for Azure](#)
[About the Framework](#)
[What's new](#)
[Scenarios](#)
[Adoption journeys](#)
[Strategy](#)
[Plan](#)
[Ready](#)
[Adopt](#)
[Govern](#)
[Manage](#)
[Secure](#)
[Organize](#)
[Resources](#)

[Learn](#) / [Azure](#) / [Cloud Adoption Framework](#) / [Get started](#) / [Feedback](#)

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

Article • 04/03/2025 • 34 contributors

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

Azure / Projects / Azure Landing Zones Public Roadmap

Type to search

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

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

What we have parked... 3

Draft
'Enterprise-Scale' rename to 'Azure Landing Zones' (repos)
Low X-Large

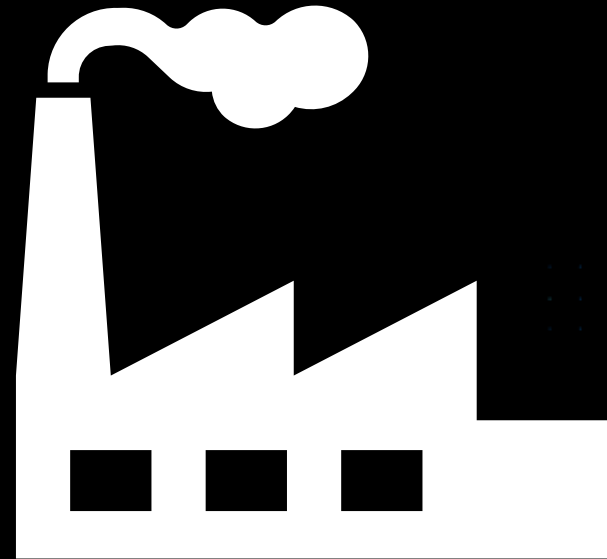
Draft
Log analytics design refresh for ALZ
Medium X-Large

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

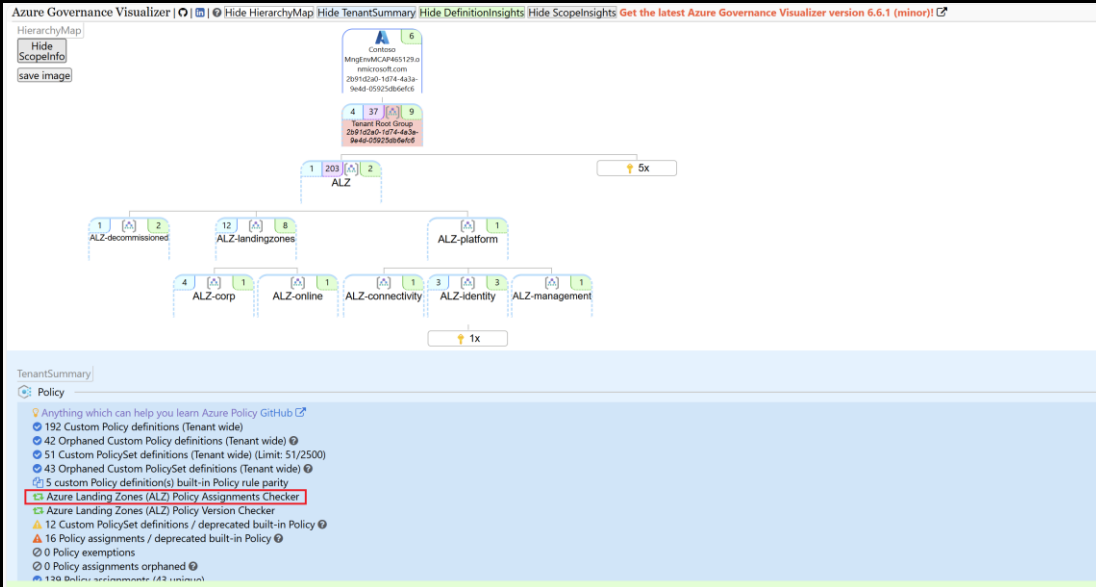
📋 We are thinking about

- 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

AzGovViz ALZ Policy Assignments Checker



How to keep up with ALZ policy releases ?



Azure Landing Zones (ALZ) Policy Assignments Checker

Azure Landing Zones (ALZ) GitHub

Download CSV semicolon | comma

Rows: 44

Clear			Clear		
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

7e5d55 Azure-Landing-Zones-Library / alz / policy_assignments / Enable-DDoS-VNET.alz_policy_assignment.json

3 people feat: update platform/alz library (automated) (#76) ✓

ebd056 last month History

```
1 {
2   "type": "Microsoft.Authorization/policyassignments",
3   "apiVersion": "2019-06-01",
4   "name": "Enable-DDoS-VNET",
5   "location": "8(default_location)",
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    "policyDefinitions": [
14      {
15        "providers": "Microsoft.Authorization/policydefinitions/94de2a03-ebc1-4caf-ad78-5d475bc83d3d",
16        "enforcementStatus": "Default",
17        "parameters": {
18          "ddoSPlan": {
19            "value": "/subscriptions/00000000-0000-0000-000000000000/resourceGroups/placeholder/providers/Microsoft.Network/ddosprotectionPlans/placeholder"
20          }
21        },
22        "effect": {
23          "value": "Modify"
24        }
25      }
26    ],
27    "scope": "/providers/Microsoft.Management/managementGroups/placeholder",
28    "notScopes": []
29  }
30 }
```

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	94de2a03-ebc1-4caf-ad78-5d475bc83d3d
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 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 4d97b09b-164f-4787-a291-c57834d21267
Rule aliases	Id (2) Alias Namespace ResourceType Path PathIsDefault DefaultPath Modifiable

New Feature: AzResourceTypesAdvertiser



HOME POLICY INITIATIVE ALIAS COMPLIANCE RESOURCE TYPES AZURE ACCESS CONTROL ENTRA-ID ACCESS CONTROL CATCHUP ⓘ										
AzResourceTypesAdvertiser 🕒 last sync: 2025-May-05 19:52:12 Etc/UTC Clear all filters 🗑️										
RT [Resource type] base	RP [Resource Provider] details									
	RP Aliases and Azure Policy					RP RBAC Operations and Roles & Roles related operation actions				
Resource type ▾	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										
compute/virtualmachines	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-4cf4efc-8124-7eba65ed3356 • Azure Regional Service Management appId:5e5e43d4-54da-4211-86a4-c6e7f37 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e0e6
compute/virtualmachines/extensions	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-4cf4efc-8124-7eba65ed3356 • Azure Regional Service Management appId:5e5e43d4-54da-4211-86a4-c6e7f37 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e0e6
compute/virtualmachines/instanceview	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-4cf4efc-8124-7eba65ed3356 • Azure Regional Service Management appId:5e5e43d4-54da-4211-86a4-c6e7f37 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e0e6
compute/virtualmachines/metricdefinitions	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-4cf4efc-8124-7eba65ed3356 • Azure Regional Service Management appId:5e5e43d4-54da-4211-86a4-c6e7f37 • Compute Artifacts Publishing Service appId:a8b6bf88-1d1a-4626-b09a729ea93c65 • Compute Recommendation Service appId:b9a92e36-2cf8-4f4e-bcb3-9d99e0e6



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	Resource types: 132
RP aliases	RP aliases: 2161
RP Azure Policy	Azure Policy definitions: 487 <ul style="list-style-type: none">if: 480then.deployment: 182then.details: 2then.existenceCondition: 0then.operations: 0
RP RBAC operations	RP RBAC operations: 279 <ul style="list-style-type: none">RP RBAC operationType action: 94RP RBAC operationType delete: 37RP RBAC operationType read: 106RP RBAC operationType write: 42
RP RBAC Roles & Operation actions	Unique RBAC Roles: 64 <ul style="list-style-type: none">RBAC Roles with action operationType: 34RBAC Roles with delete operationType: 22RBAC Roles with read operationType: 59RBAC Roles with write operationType: 30
RP related 1st party Service Principals	RP related 1st party Service Principals: 9 <ul style="list-style-type: none">Microsoft Azure Windows Virtual Machine Sign-in (Azure Windows VM Sign-In) (appId: 372140e0-b3b7-4226-8ef9-d57986796201) [JSON;CSV]Microsoft Azure Linux Virtual Machine Sign-In (Azure Linux VM Sign-In) (appId: ce6ff14a-7fdc-4685-bbe0-f6afdfcfa8e0) [JSON;CSV]Marketplace Caps API (appId: 184909ca-69f1-4368-a6a7-c558ee6eb0bd) [JSON;CSV]Compute Usage Provider (appId: a303894e-f1d8-4a37-bf10-67aa654a0596) [JSON;CSV]Compute Resource Provider (Managed Disks Resource Provider) (appId: 606ecd67-8c8c-4951-9b3c-23c25a2169af) [JSON;CSV]Compute Recommendation Service (appId: b9a92636-2cf8-4f4e-bc93-9d99a0e14ab) [JSON;CSV]Compute Artifacts Publishing Service (appId: a8b6bf88-1d1a-4626-b040-9a729ea93c65) [JSON;CSV]Azure Regional Service Manager (appId: 5e5e43d4-54da-4211-86a4-c6e7f3715801) [JSON;CSV]Azure Compute (appId: 579d9c9d-4c83-4efc-8124-7eba65ed3356) [JSON;CSV]
All Azure RPs	<ul style="list-style-type: none">Microsoft LearnAzResourceTypesAdvertiser (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 <ul style="list-style-type: none">2024-11-012024-07-012024-03-012023-09-012023-07-012023-03-012022-11-012022-08-012022-03-01
All Microsoft Azure RTs	AzResourceTypesAdvertiser
Aliases and Azure Policy	
Aliases	aliases: 287
Azure Policy	Azure Policy definitions: 392 <ul style="list-style-type: none">if: 389then.deployment: 108then.details: 2then.existenceCondition: 0then.operations: 0
RBAC Operations and Roles & Roles related operation actions	
RBAC operations	RBAC operations: 28 <ul style="list-style-type: none">RBAC operationType action: 25RBAC operationType delete: 1RBAC operationType read: 1RBAC operationType write: 1
RBAC Roles & Operation actions	Unique RBAC Roles: 41 <ul style="list-style-type: none">RBAC Roles with action operationType: 6RBAC Roles with delete operationType: 10RBAC Roles with read operationType: 38RBAC Roles with write operationType: 15
Capabilities & Locations	
Diagnostic logs	True <ul style="list-style-type: none">log-categories
Diagnostic metrics	True <ul style="list-style-type: none">metrics
Customer-managed key (CMK) [experimental]	True <ul style="list-style-type: none">Microsoft LearnEnforce Encryption with a customer-managed key (CMK) at scale
System-Assigned-Resource-Identity	True
Cross-ResourceGroup-Resource-Move	True
Cross-Subscription-Resource-Move	True
Assessment tooling	
Azure Advisor	Azure Advisor recommendations: 80 <ul style="list-style-type: none">Cost [High] Right-size or shutdown underutilized virtual machinesCost [Medium] Rock recommendation type for kusto-based ingestionHighAvailability [High] Migrate workload to D-series or better virtual machineHighAvailability [High] Standard_NC24rs_v3 virtual machine (VM) size in NCv3-series is being retired.HighAvailability [High] Update your outbound connectivity protocol to Service Tags for Azure Site RecoveryHighAvailability [High] Upgrade to a newer offer of Virtual Machine imageHighAvailability [High] Upgrade to a newer SKU of Virtual Machine imageHighAvailability [High] Upgrade VM from Premium Unmanaged Disks to Managed Disks at no additional costHighAvailability [High] Upgrade your deprecated Virtual Machine image to a newer image
Azure Proactive Resilience Library v2 (APRLv2)	Azure Proactive Resilience Library v2 recommendations: 18 <ul style="list-style-type: none">DisasterRecovery [High] Validate VM functionality with a Site Recovery test failover to check performance at targetDisasterRecovery [Medium] Replicate VMs using Azure Site RecoveryDisasterRecovery [Medium] Reserve Compute Capacity in Disaster Recovery RegionsDisasterRecovery [Medium] Backup VMs with Azure Backup serviceHighAvailability [High] Reserve Compute Capacity for critical workloadsHighAvailability [High] Use maintenance configurations for the VMsHighAvailability [High] Run production workloads on two or more VMs using VMSS FlexHighAvailability [High] Use Managed Disks for VM disks
PSRule for Azure	PSRule for Azure rules: 19 <ul style="list-style-type: none">Cost Optimization [Awareness] Multi-tenant Hosting RightsCost Optimization [Awareness] Use Azure Hybrid BenefitCost Optimization [Awareness] Use current VM SKUsCost Optimization [Important] VMs should not be stopped stateOperational Excellence [Awareness] Use valid VM computer namesOperational Excellence [Awareness] Use valid VM namesOperational Excellence [Important] Migrate to Azure Monitor AgentOperational Excellence [Important] Use Azure Monitor AgentOperational Excellence [Important] Virtual Machine agent is not provisioned
Azure Quick Review (AZQR)	Azure Quick Review (AZQR) recommendations: 25 <ul style="list-style-type: none">DisasterRecovery [Medium] Backup VMs with Azure Backup serviceDisasterRecovery [Medium] Replicate VMs using Azure Site RecoveryGovernance [Low] Ensure that your VMs are compliant with Azure PoliciesGovernance [Low] Review VMs in stopped stateGovernance [Low] Virtual Machine Name should comply with naming conventionsGovernance [Low] Virtual Machine should have tagsHighAvailability [High] Deploy VMs across Availability ZonesHighAvailability [High] Migrate VMs using availability sets to VMSS FlexHighAvailability [High] Reserve Compute Capacity for critical workloads
Infrastructure as Code (IaC)	
ARM (Azure Resource Manager) templates	ARM (Azure Resource Manager) template API versions: 26 <ul style="list-style-type: none">latest2024-11-012024-07-012024-03-012023-09-012023-07-012023-03-012022-11-012022-08-012022-03-01
Bicep templates	Bicep template API versions: 26 <ul style="list-style-type: none">latest2024-11-012024-07-012024-03-012023-09-012023-07-012023-03-012022-11-012022-08-012022-03-01
Terraform providers	Terraform providers: 6 <ul style="list-style-type: none">linux.virtual.machine

Azure Verified Modules (AVM) Bicep

Azure Verified Modules (AVM) Terraform

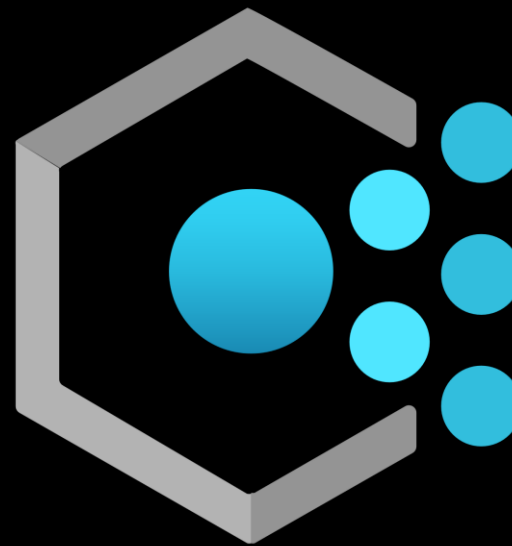
Virtual Machine

- 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



aka.ms/amba/alz/whatsnew

- 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

- **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) for 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 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 ALZ 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

Draft

Azure Monitor Ingestion limit alert

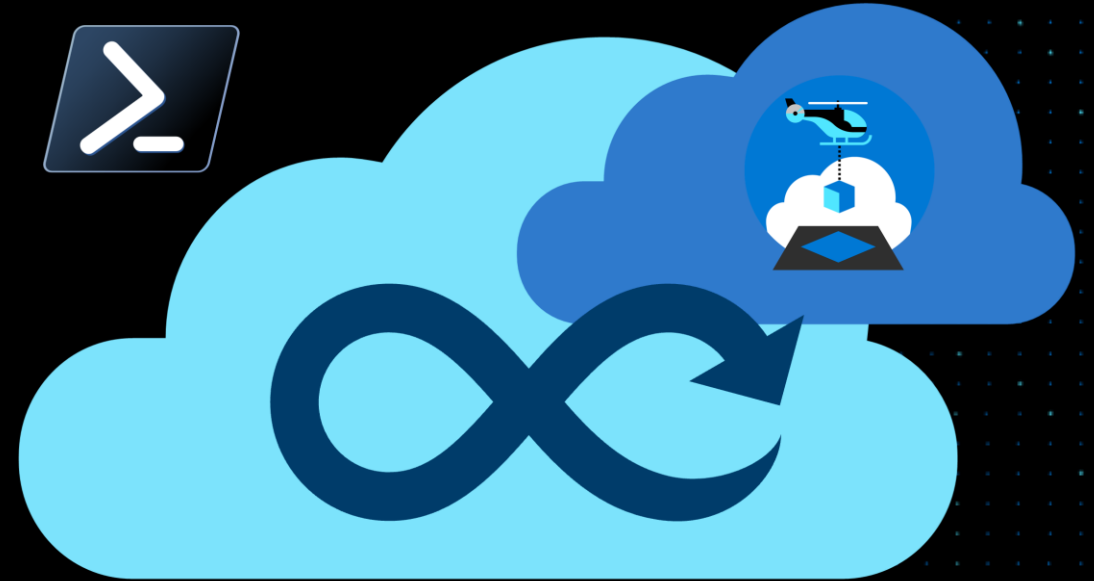
Medium Medium ALZ



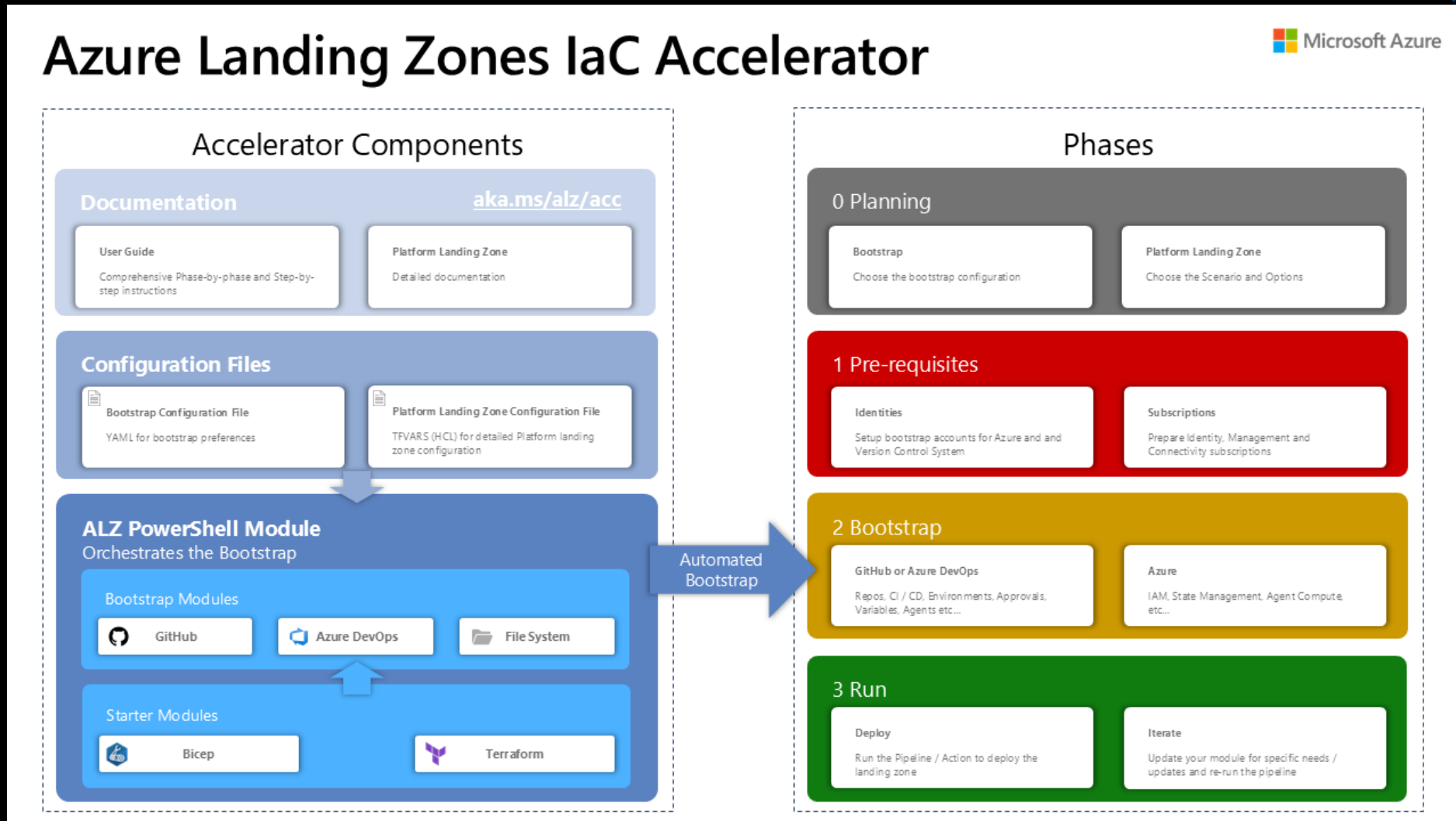


ALZ IaC Accelerator Updates

aka.ms/alz/acc



How the ALZ IaC Accelerator Works?



aka.ms/alz/acc



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)



All subject to testing and validation
Migration will be non-disruptive for all resources
You can continue deploying workloads
Two stages of migration: <ul style="list-style-type: none">• Subscription move to a new management group• Terraform state migration for management and connectivity resources

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!](#)



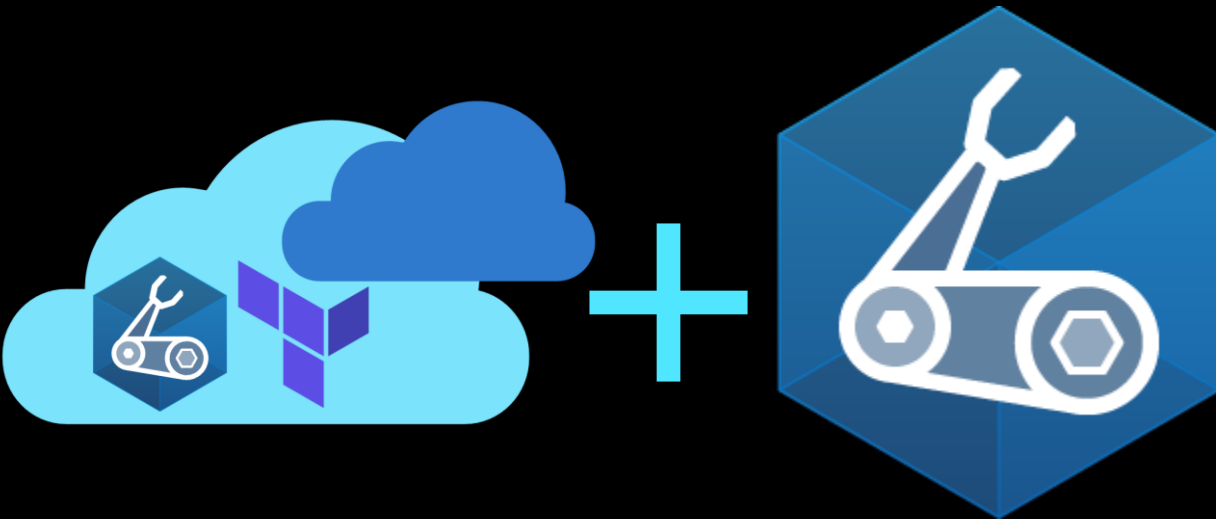


Bicep Azure Verified Modules for Platform Landing Zones (ALZ)| Update



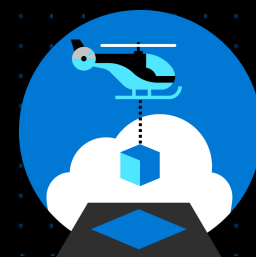
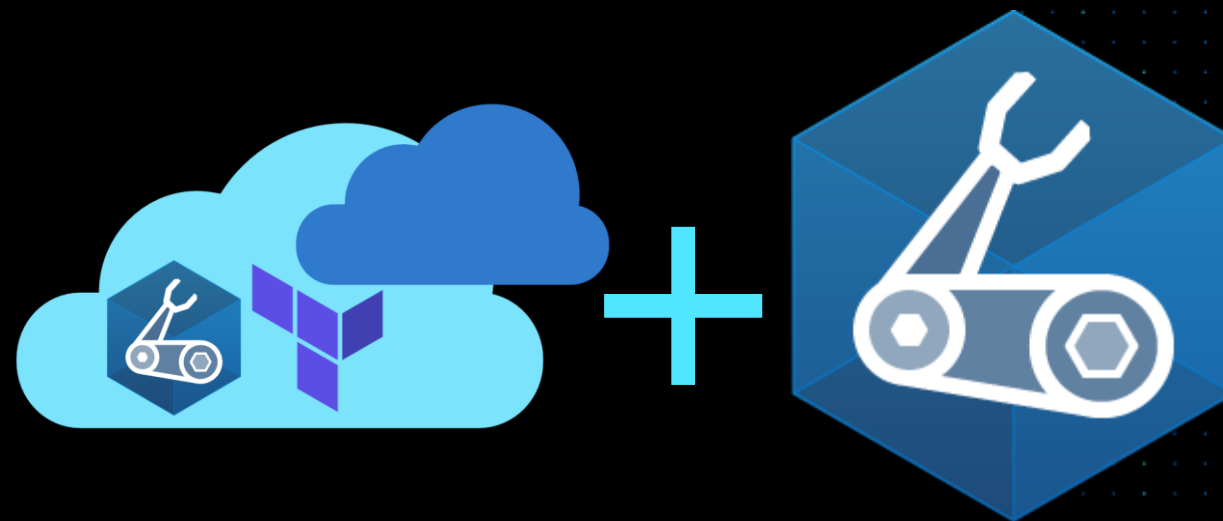
- See [An Update on Bicep Azure Verified Modules for Platform Landing Zone \(ALZ\) | Microsoft Community Hub](#)
- **Soft Launch Target:** June–July 2025
- Preview Available: [`avm/ptn/alz/empty`](#)
 - ["Max"](#) Test case for depth example
- Coming Soon (based on [feedback](#))

- ``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

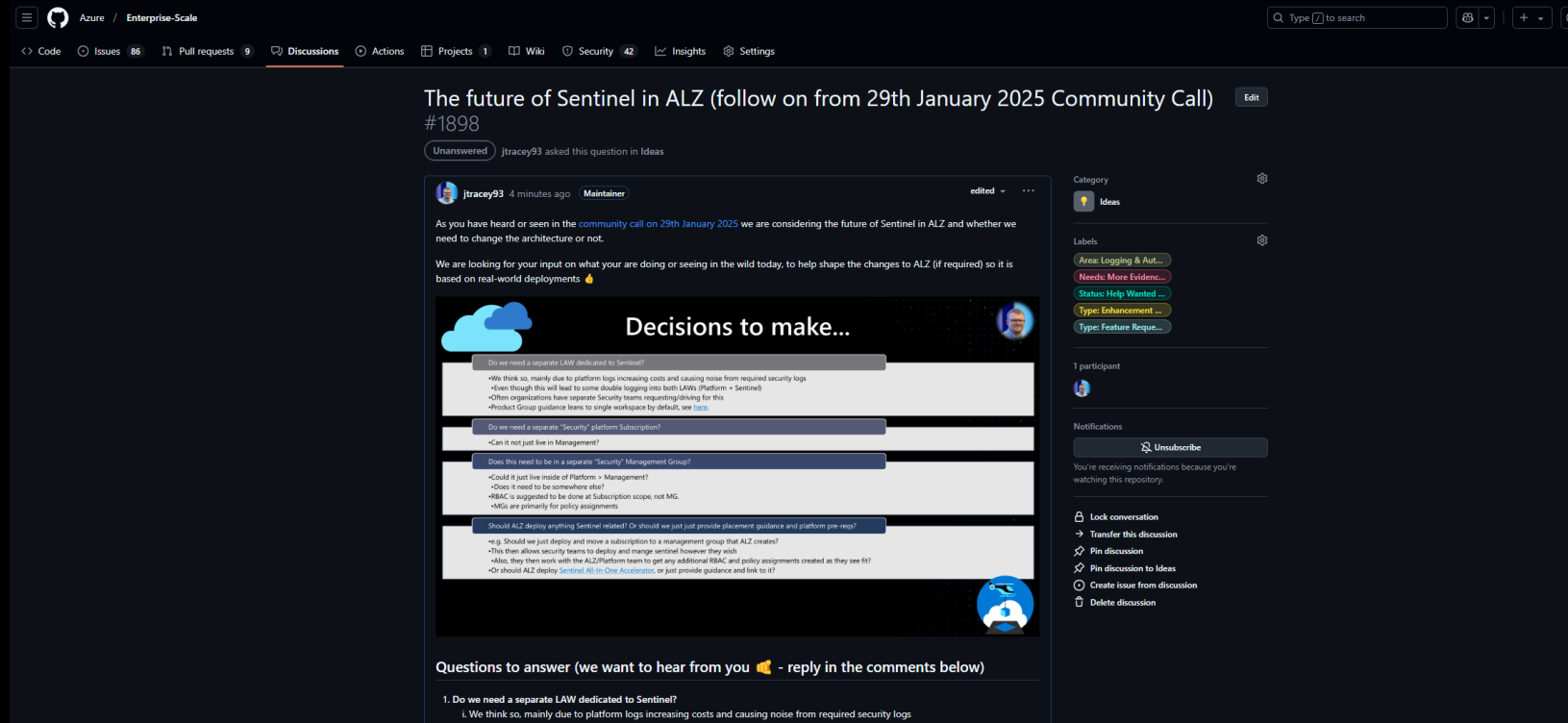




Thanks for all your feedback on



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



The screenshot shows a GitHub discussion page for the repository `Azure/Enterprise-Scale`. The discussion is titled "The future of Sentinel in ALZ (follow on from 29th January 2025 Community Call)" and is labeled with the number #1898. It is categorized as an "Idea" and has a status of "Unanswered". The discussion was started by user `jtracey93` 4 minutes ago. The main content of the discussion is a document titled "Decisions to make..." which lists several questions and considerations regarding the future of Sentinel in ALZ. The document is structured with a title, a list of questions, and a list of considerations. The questions are: "Do we need a separate LAW dedicated to Sentinel?", "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?", and "Should ALZ deploy anything Sentinel related? Or should we just provide placement guidance and platform pre-req?". The considerations include: "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 requiring driving for this", "Product Group guidance leans to single workspace by default, see [here](#)", "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", "MSOs are primarily for policy assignments", "If so, 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?", and "Or should ALZ deploy Sentinel in One Architecture, or just provide guidance and link to it?". The discussion also includes a section titled "Questions to answer (we want to hear from you)" with a prompt to reply in the comments below. On the right side of the discussion, there are options to lock the conversation, transfer the discussion, pin the discussion, pin the discussion to ideas, create an issue from the discussion, and delete the discussion. There is also a notification section indicating that the user is receiving notifications because they are watching this repository.





We now have a proposal to implement 👍



github.com/Azure/Enterprise-Scale/discussions/1978
(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

Are you happy with the proposal?

Yes ☑

91%

No (please leave comment below as to why 👍)

8%





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

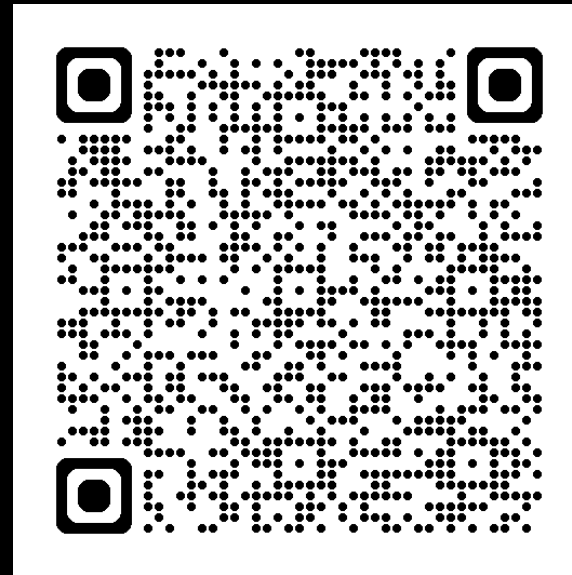


Next Community Call will 17th September 2025



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