This meeting is being recorded

Before we get started...

At any point, if you have a question please put it in the chat!
(we have members of the team here to help 😎)
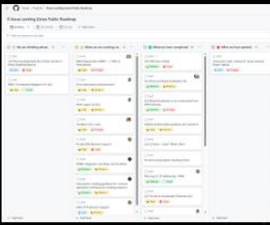
Also we may stop and discuss your question/point at that time, we want this to be an open discussion with all of you 🙂

Implementation Options & Accelerators

ALZ Public Roadmap

aka.ms/ALZ/Roadmap

ALZ What's New?

https://aka.ms/ALZ/WhatsNew

Single place to stay up-to-date

Policy Refresh H2FY24 Updates

MMA Deprecation Update

AMBA Updates

AzAdvertizer Updates

Multi-Region Updates

Zone Redundancy Updates

Microsoft Cloud for Sovereignty Updates

ALZ Terraform vNext Update

ALZ Bicep Updates

Implementation Options & Accelerators 🏗️ 🏎️

Accelerators

Platform

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

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

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

Cloud operating model roles and responsibilities

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

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

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

Application

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

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

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

Subscription Vending

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

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

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

aka.ms/ALZ/AAC

ALZ What's New?

https://aka.ms/ALZ/WhatsNew

Single place to stay up-to-date

Updates

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

June 2024

Policy

- Added new custom policy Do not allow deletion of specified resource and resource type that provides a safeguard against accidental removal of the User Assigned Managed Identity used by AMA. Assigned at the Platform Management Group, it blocks delete calls using the deny action effect.

🆕 AMA Updates

The ALZ Portal Accelerator has been enhanced with the latest AMA updates, ensuring a seamless and efficient management experience. 🚀

Key updates include:

- Azure Landing zones is now using a single centralized User Assigned Managed Identity. The centralization of User Assigned Managed Identity for Azure Monitor Agent (AMA) marks a significant advancement in our ability to manage large-scale deployments efficiently.
    - The User Assigned Managed Identity `id-ama-prod-<location>-001` is created in resource group `<enterpriseScaleCompanyPrefix>-mgmt` in the management subscription or in the platform subscription when selecting 'Single' in the Platform subscription options.
    - The feature flag `restrictBringYourOwnUserAssignedIdentityToSubscription` has been added to the policies and initiatives that enables the use of a single centralized User Assigned Managed Identity.
        - `restrictBringYourOwnUserAssignedIdentityToSubscription` set as True (Policy/Initiative default): Restricts the bring your own UAMI to a UAMI from the same subscription as the VM.
        - `restrictBringYourOwnUserAssignedIdentityToSubscription` set as False (**ALZ Default**): Removes that restriction and allows you to assign your own UAMI from any subscription within the tenant/ scope of assignment.
    - We've updated the following built-in policy initiatives to support single User Assigned Managed Identities:
        - Enable Azure Monitor for VMs with Azure Monitoring Agent(AMA)
        - Enable Azure Monitor for VMSS with Azure Monitoring Agent(AMA)
        - Configure SQL VMs and Arc-enabled SQL Servers to install Microsoft Defender for SQL and AMA with a user-defined LA workspace
        - [Preview]: Enable ChangeTracking and Inventory for virtual machines
        - [Preview]: Enable ChangeTracking and Inventory for virtual machine scale sets
- Custom Defender for SQL initiative has been deprecated and is replaced by Configure SQL VMs and Arc-enabled SQL Servers to install Microsoft Defender for SQL and AMA with a user-defined LA workspace
- Custom User Assigned Managed Identity policy has been deprecated. UAMI for AMA is now centrally deployed therefore this policy is no longer required.

New Doc Move

Networking – AVNM

Azure Virtual Network Manager in Azure Landing Zones

The Azure Landing Zones conceptual architecture recommends one of two networking topologies: an Azure Virtual WAN-based network topology or a network topology based on a traditional hub and spoke architecture. As the business requirements change over time (for example, migration of on-premises applications to Azure that requires hybrid connectivity), AVNM allows you to expand and implement networking changes, in many cases, without disrupting what is already deployed in Azure.

Azure Virtual Network Manager allows you to create three types of topologies across subscriptions for both existing and new virtual networks:

- Hub and spoke topology
- Hub and spoke topology with direct connectivity
- Mesh topology (Preview)
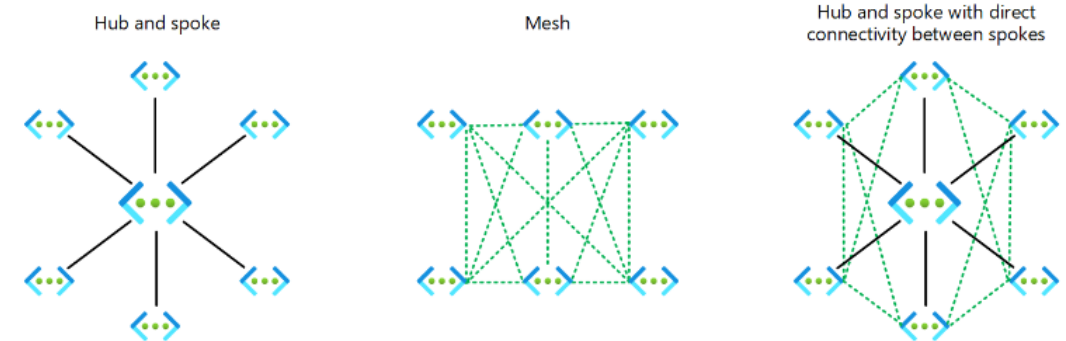
ⓘ Note

Azure Virtual Network Manager does not support Azure Virtual WAN hubs as part of a network group or as the hub in a topology. For more information, see Azure Virtual Network Manager FAQ.

Doc Update

Application Environments in ALZ

Private Link and DNS integration at scale

> ① **Note**
>
> You can deploy a DNS Private Resolver in your Hub Virtual Network alongside your ExpressRoute Gateway etc. However, you must ensure that resolution of public FQDNs is permitted and replies with a valid response via a DNS Forwarding Ruleset Rule to the targeted DNS server. As some Azure services rely upon rely upon the ability to resolve public DNS names to function. See more here

Announcement

Bicep Subscription Vending Module now migrated to AVM Pattern Module as v0.1.0 (avm/ptn/lz/sub-vending) 🥳

Original `v1.5.2` becomes `v0.1.0` in AVM

Policy Refresh H2FY24 Updates
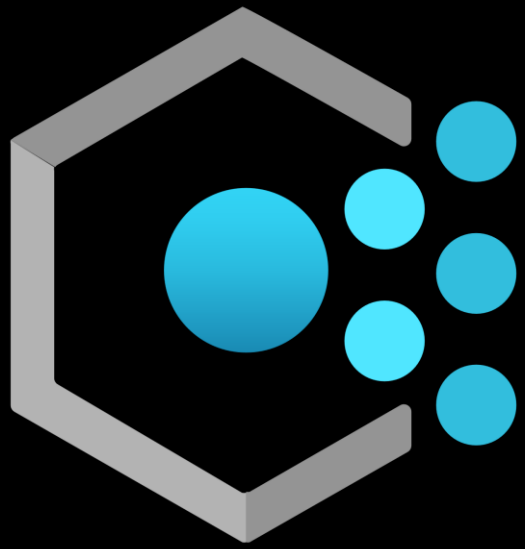
ALZ Policy News

aka.ms/alz/whatsnew

- ## Policy Refresh H2 FY24
  - Massive update - be sure to review "What's New"
  - No "breaking" changes!

- ## Diagnostic Settings v2 🎉
  - Transitioned to new built-in initiative and 140+ resources covered
  - Deprecated all ALZ custom policies and initiative
  - Raise any gaps on repo "Discussions" topic

- ## Trusted Launch
  - New Trusted Launch initiative to audit compliance

- ## Private DNS Zones
  - Added several resources with built-in policies
  - *New* generic custom policy to enable for all supporting resources

- ## Backup
  - New backup initiative auditing
    - Immutability
    - Soft Delete
    - Multi-User Authorization

Many other updates!

ALZ Policy News

- ## Workload Specific Compliance

  - New component for ALZ

  - Common enhanced controls for highly regulated industries (FSI, healthcare, etc)

  - Separate section in portal accelerator

    - 25 new custom initiatives

    - 24 new custom policies

    - Significant updates to existing initiatives

  - Coming soon to Terraform/Bicep

- ## Defender for Cloud

  - Fixes due to DfC API breaking changes

    - API

    - Security Contacts

  - New Endpoint protection policy assignment at subscription level

- ## Loads of documentation updates in the Wiki

MMA Deprecation Update

MMA Deprecation

- ALZ is now using a single centralized User Assigned Managed Identity for AMA

- Built-in Policies:

  - Centralized UAMI feature added to:
    - VM Insights
    - Change Tracking
    - Microsoft Defender for SQL

  - Microsoft Defender for SQL:
    - Bring your own UAMI
    - Bring your own DCR
    - Transitioned to use the updated built-in policy

- Custom Policies

  - Added a Deny Action Delete policy to protect the UAMI for AMA from accidental deletion.

- Deprecated Policies:

  - Custom Defender for SQL initiative has been deprecated and is replaced by Configure SQL VMs and Arc-enabled SQL Servers to install Microsoft Defender for SQL and AMA with a user-defined LA workspace

  - Custom User Assigned Managed Identity policy has been deprecated. UAMI for AMA is now centrally deployed therefore this policy is no longer required.

MMA Deprecation

- Coming June 2024:

  - AMA for Bicep and Terraform

  - Brownfield guidance on updating existing ALZ deployments to use AMA

AMBA Updates

AMBA Updates

aka.ms/amba/patterns/alz

- Alert Processing Rule for alert suppression

- Bring your own Action Group and/ or Alert Processing Rule

- Alerts for Arc-enabled VMs

- Documentation updates, Architecture Diagram updated (Visio)

- Preparing for the unexpected: Azure Incident Readiness

  - Preparing for the unexpected: Azure Incident Readiness (youtube.com)

- Feature Update: Azure Action Groups - Email Azure Resource Manager role

  - In the new behavior, the users who inherit a role assignment from being a group member will start receiving emails.

AMBA Roadmap

aka.ms/amba/patterns/alz

- AMBA ALZ Portal Accelerator

- Quota Alerts

- Alignment with APRLv2

- Update AMBA release in the ALZ Portal Accelerator

- AMBA for ALZ Bicep/ Terraform

  - 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

- Azure Site Recovery (ASR) now surfaces default alerts via Azure Monitor for critical events.

  - These alerts will be added to AMBA ALZ Pattern.

- Adding alerts for ManagedHSM

- Refactoring MonitorDisable

AzAdvertizer Updates

Multi-Region Updates

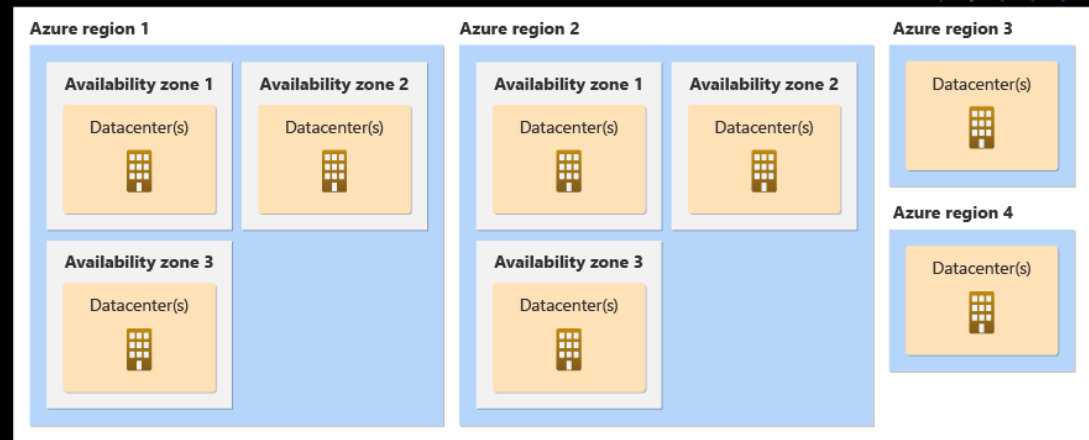| Azure region 1		Azure region 2		Azure region 3
Availability zone 1 Datacenter(s)	**Availability zone 2** Datacenter(s)	**Availability zone 1** Datacenter(s)	**Availability zone 2** Datacenter(s)	Datacenter(s)
Availability zone 3 Datacenter(s)		**Availability zone 3** Datacenter(s)		**Azure region 4** Datacenter(s)
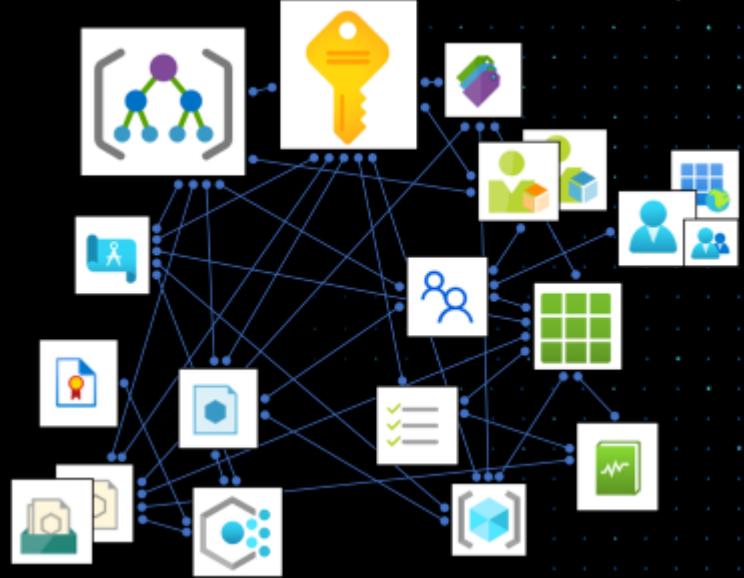
Multi-Region Updates

- We've updated a number of CAF ALZ documents

- ALZ Portal update planned this month!

  Azure landing zone accelerator   ...
  Deploy from a custom template

  Resource prefix (Root ID) * ⓘ   [   ]

  Platform subscription options ⓘ   ◉ Dedicated (recommended)
                                      ○ Single

  Deploy in a secondary region ⓘ   ◉ Yes (recommended)
                                      ○ No

- Bicep and Terraform planned CY2024 Q3

Azure Virtual Network Manager in Azure landing zones

Define an Azure network topology

Define your tagging strategy

Resource naming and tagging decision guide

Traditional Azure networking topology

Landing zone regions

Hybrid identity with Active Directory and Microsoft Entra ID in Azure landing zones
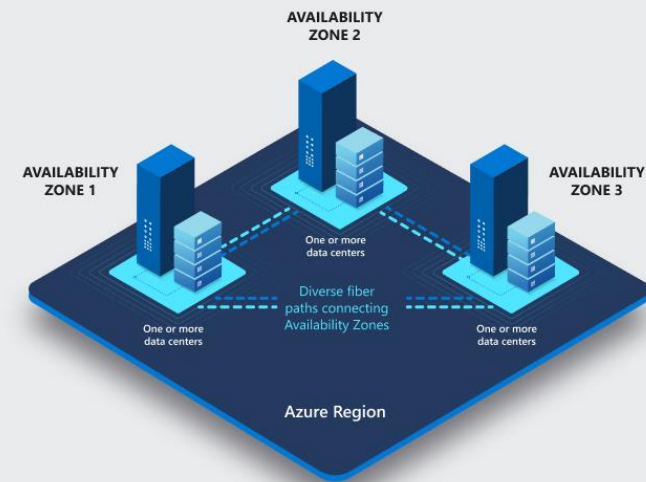
Management groups

Subscription considerations and recommendations

Resource organization design area overview

Zone Redundancy Updates

Zone Redundancy Updates

- ## Phased Approach

  - ~~Phase 1 – Portal, Bicep and Terraform *Accelerators* zone redundant by default by end of Q2 CY24~~

  - Phase 2 – Bicep and Terraform Modules zone redundant by default by end of CY24

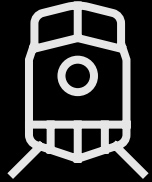- ## Combined Blog with Multi-Region to follow

Microsoft Cloud for Sovereignty Updates

# Microsoft Cloud for Sovereignty | Release Wave 1, April 2024

Guardrails

SLZ is more powerful with more **configurability** and leveraging an **Azure built-in Sovereign Policy Baseline**.

Additional sovereign controls enable additional compliance needs, including policy initiatives for **NATO**, policies to leverage **Trusted Launch VMs**, and updates for **Italy ACN** and **NL BIO**.

Additional Azure services available in GSP, including managed HSM.
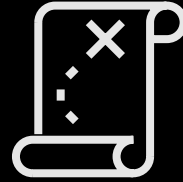
Guidance

Significant additional sovereign guidance around **workload migration** and CAF/WAF/CSA Plays

New **LLM reference architecture** for AI workloads

Introduction of first guidance around sovereign **M365** and **D365** configurations
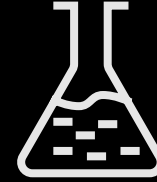
Previews

New tools available for **assessing** existing environments and monitoring for **drift** enter public previews

Development continues Azure **portal experiences** enabling easier discovery and new capabilities for private preview customers today

Find out more at: Streamline controls with Microsoft Cloud for Sovereignty - Microsoft Industry Blogs

ALZ Terraform
vNext Update

Pathway to v1.0.0

Decouple ALZ library and module/provider ✅

Override archetypes in library ✅

Policy assignment modification in HCL ✅

Architecture definition as code
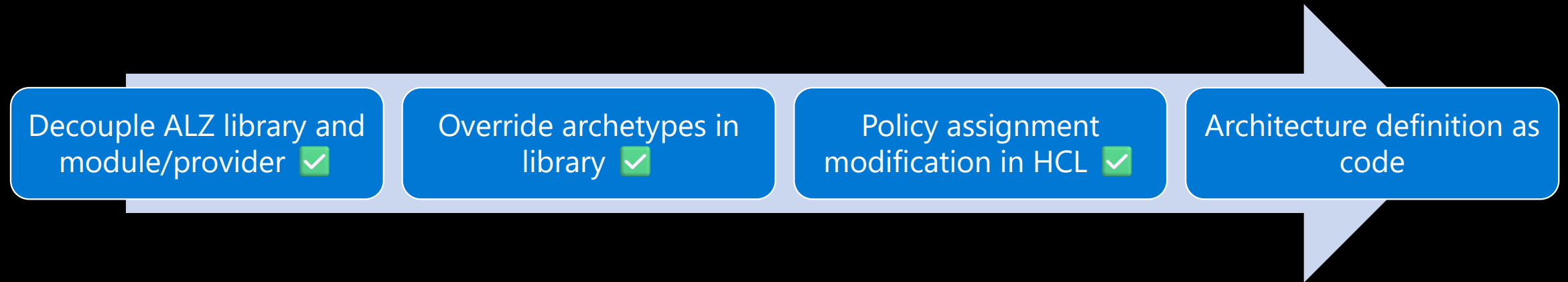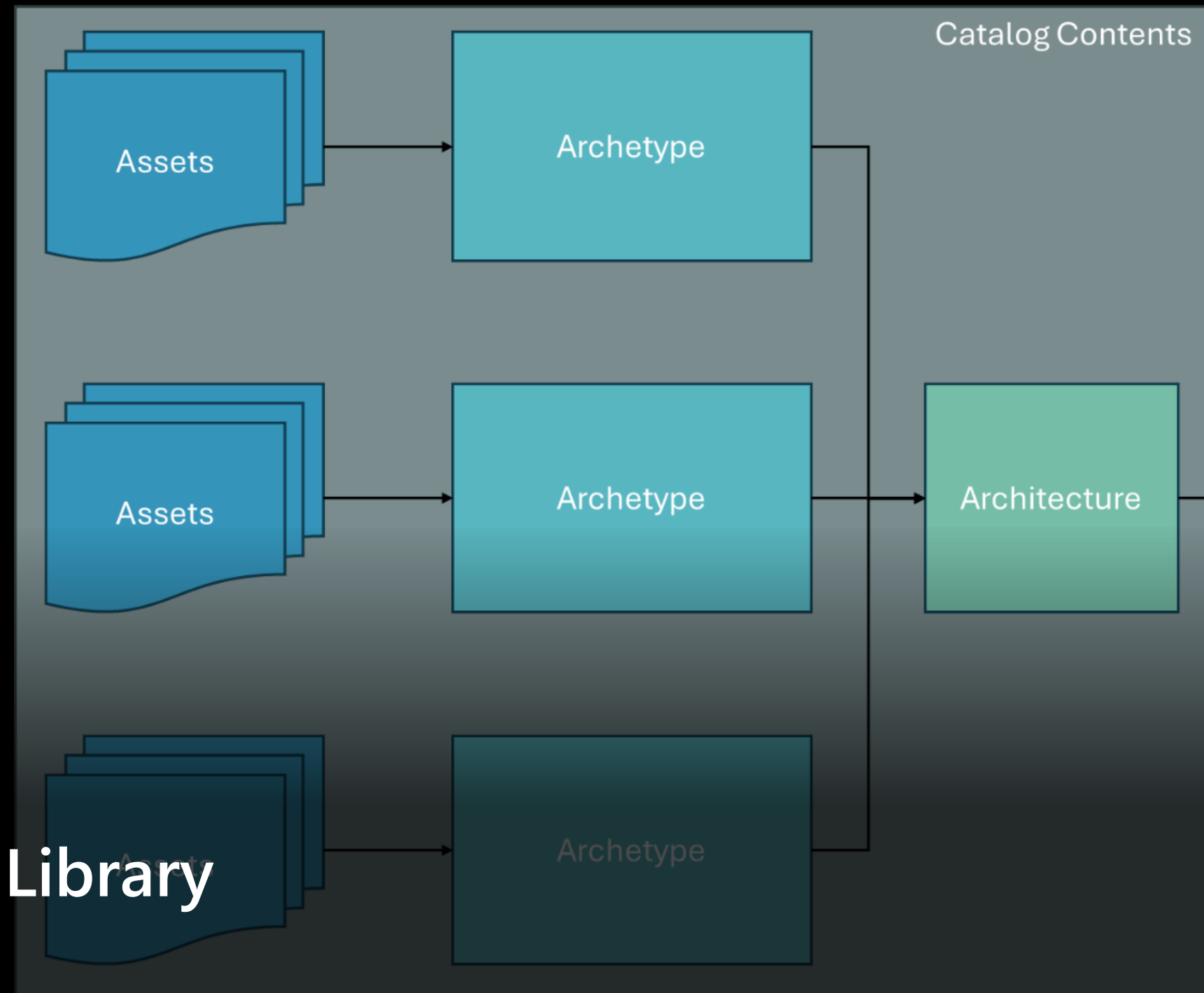
Architecture-as-code

Before

- Define MG architecture in HCL

After

- Define architecture as file
- Can either take one from our library, e.g. ALZ default
- Or create your own

Example file

```yaml
---
name: alz
management_groups:
  - name: orgroot
    display_name: "Org Root"
    pre_existing: true
    archetypes:
      - root
      - fsi_root
    children:
      - landing_zones
      - platform
      - sandbox
  - name: landingzones
    display_name: "Landing Zones"
    pre_existing: false
    archetypes:
      - landing_zones
    children:
      - corp
      - online
```

ALZ Bicep Updates

ALZ-Bicep Updates

v0.17.3 and v0.17.4 just released!

- Availability zones supported when running the Accelerator.

- Added policy exemption module for baseline Sovereign Landing Zone initiatives.

- Multiple bug fixes specific to the networking modules as well as one bug for the ALZ default policy assignments module.

- Documentation additions and improvements including but not limited to:

  - Guidance for integrating Azure Monitor Baseline Alerts within the Accelerator framework.

  - Wiki page created for providing a list of Known Issues within ALZ-Bicep

ALZ-Bicep Roadmap

Public Roadmap

- Ingest Policy Refresh FY24H2

- Updates to accommodate MMA Deprecation with AMA.

- Integrate Azure Monitor Baseline Alerts and associated documentation.

- Automate the setup of Azure DevOps and GitHub within the Accelerator.

- Simplify policy updates and customizations within the Accelerator framework.

- Migrate to be built from AVM modules 👀
  (more info on next slide)

ALZ-Bicep "Migration" to AVM

- **What This Means for ALZ-Bicep?**
  - Put very simply, all ALZ Bicep modules will be deprecated and instead a new version of ALZ Bicep will be released that will be built solely of AVM Bicep modules (Resource & Pattern). The ALZ Bicep repo will transition to become the home of the accelerator providing examples and reference code bases of how to deploy the various ALZ reference architectures.
- **Transition Plan**
  - Whether ALZ Bicep Team maintained or not, they will all live in AVM as their home.
  - We will provide detailed steps, and possibly tooling, to ensure a smooth transition.
- **Benefits for You**
  - Enhanced customization & greater flexibility to tailor modules, via input parameters, to your specific needs as the AVM modules are way more flexible by design.

- Enhanced specifications/standards, testing, CI framework to benefit from promoting consistency and quality further in the modules that build ALZ Bicep.
- Closer alignment with the Well-Architected Framework as this is an AVM requirement.
- Larger community to help implement feature requests and fix any bugs.
- Breaking up some of the monolithic modules into smaller pieces, e.g. Hub Network ALZ Bicep module will be no more and instead composed of various AVM Resource Modules.

ALZ-Bicep "Migration" to AVM

AVM Maintained Modules (Already exist unless stated)

Governance Modules

Management Groups (inc. Diag Settings)
(avm/res/management/management-group)

Subscription Placement
Requires creation/development

ALZ Custom Policy Definitions & Initiatives
Pattern requires creation/development

Custom Policy Definitions & Initiatives
Resource/Pattern requires creation/development

ALZ Default Policy Assignments
Pattern requires creation/development

Policy Assignments
(avm/ptn/authorization/policy-assignment)

ALZ Custom Role Definitions
Resource/Pattern requires creation/development

Custom Role Definitions
Resource/Pattern requires creation/development

Role Assignments
(avm/ptn/authorization/role-assignment)

Logging & Monitoring Modules

Log Analytics Workspace
(avm/res/operational-insights/workspace)

Log Analytics Workspace Solution
(avm/res/operational-insights/solution)

Hub Networking Replacement Modules

Virtual Network
(avm/res/network/virtual-network)

Azure Firewall
(avm/res/network/azure-firewall)

Azure Firewall Policy
(avm/res/network/firewall-policy)

Private Link Private DNS Zones
(avm/ptn/network/private-link-private-dns-zones)
Under Development

VPN/ExpressRoute Gateway
(avm/res/network/virtual-network-gateway)

Azure Bastion
(avm/res/network/bastion-host)

VWAN Networking Replacement Modules

Azure Firewall
(avm/res/network/azure-firewall)

Private Link Private DNS Zones
(avm/ptn/network/private-link-private-dns-zones)
Under Development

VPN Gateway
(avm/res/network/vpn-gateway)

ExpressRoute Gateway
(avm/res/network/express-route-gateway)

Virtual WAN
(avm/res/network/virtual-wan)

Virtual WAN Hub
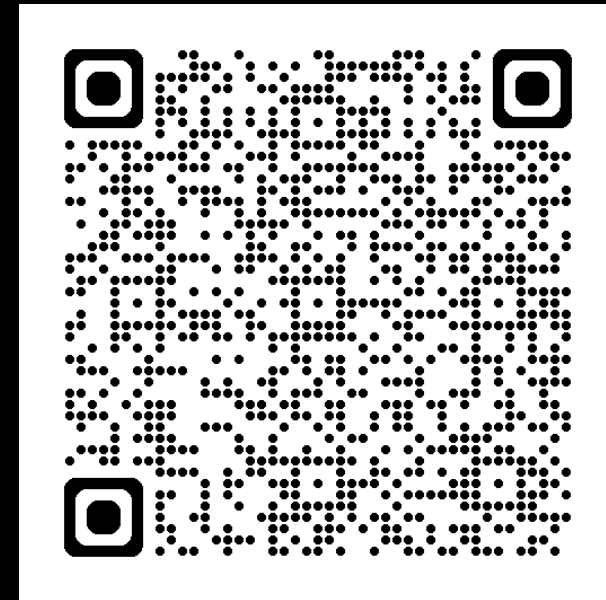(avm/res/network/virtual-hub)

Feedback Link!

Q & A

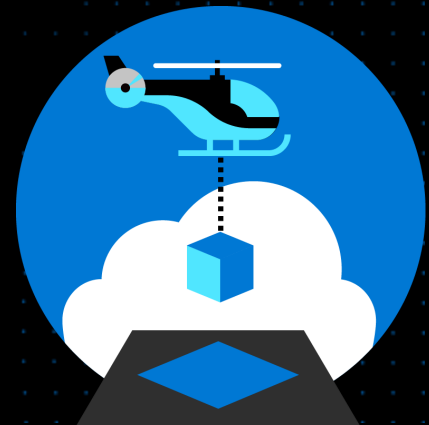Next Community Call will be on 25th September 2024 👍

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

Stay tuned to issue #1666 (ALZ/ESLZ Repo)

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

This month's presenters:

Microsoft

Thank You! 👋

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