This month’s presenters:

Microsoft

Azure Landing Zones

5th November 2025 - External Community Call

Registration:
aka.ms/ALZ/CommunityCall

Agenda (please add suggestions):
aka.ms/ALZ/CommunityCallAgenda

Microsoft

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.

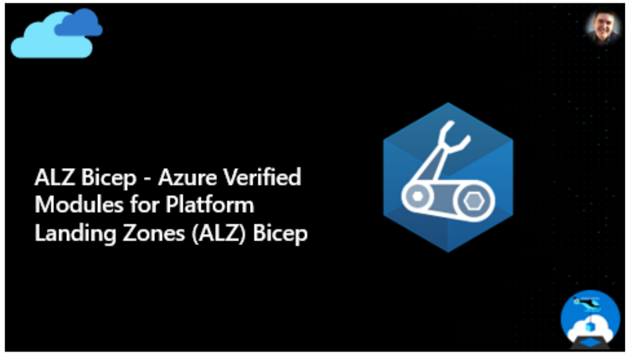
This meeting is being recorded

Before we get started...

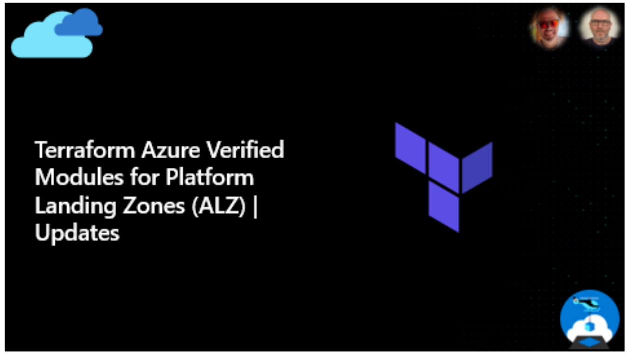
At any point, if you have a question please put it in the chat!

(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 🥹



ALZ Bicep - Azure Verified Modules for Platform Landing Zones (ALZ) Bicep



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

ALZ Library Overview & Deep Dive

ALZ IaC Accelerator Updates

Portal & Policy Refresh H1 FY26 Updates

ALZ MS Learn & Other Updates

Sovereign landing zone

AMBA-ALZ Updates
aka.ms/amba/alz

AI Landing Zone Accelerator for AI Apps & Agents

ALZ Bicep - Azure Verified Modules for Platform Landing Zones (ALZ) Bicep

ALZ-Bicep | Updates

- Release of v0.23.1!
  - Networking related enhancements and bug fixes
    - Add Virtual Network Gateway UDT with allowed values for clarity
    - Support for additional DNS zones beyond the defaults.
- Some other updates from other releases as of the last community call:
  - Updated policy set and assignments for the second half of FY25
  - Sidecar network to support additional VWAN topologies
  - Now allow individual policies to be set to DoNotEnforce.

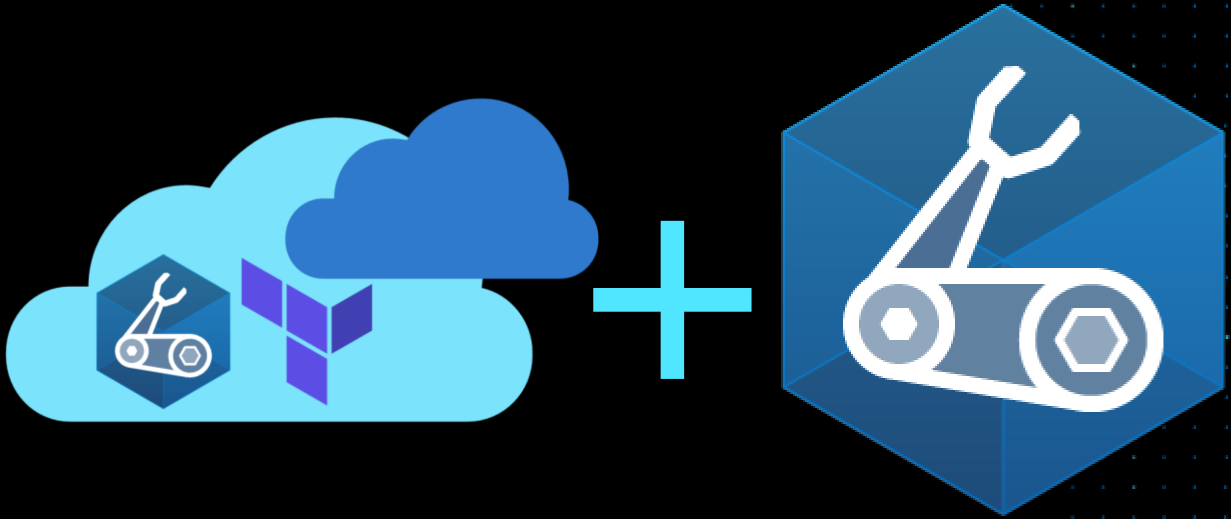
📌 See full release notes from all releases here!

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

Release Coming Soon – In final prep for public preview

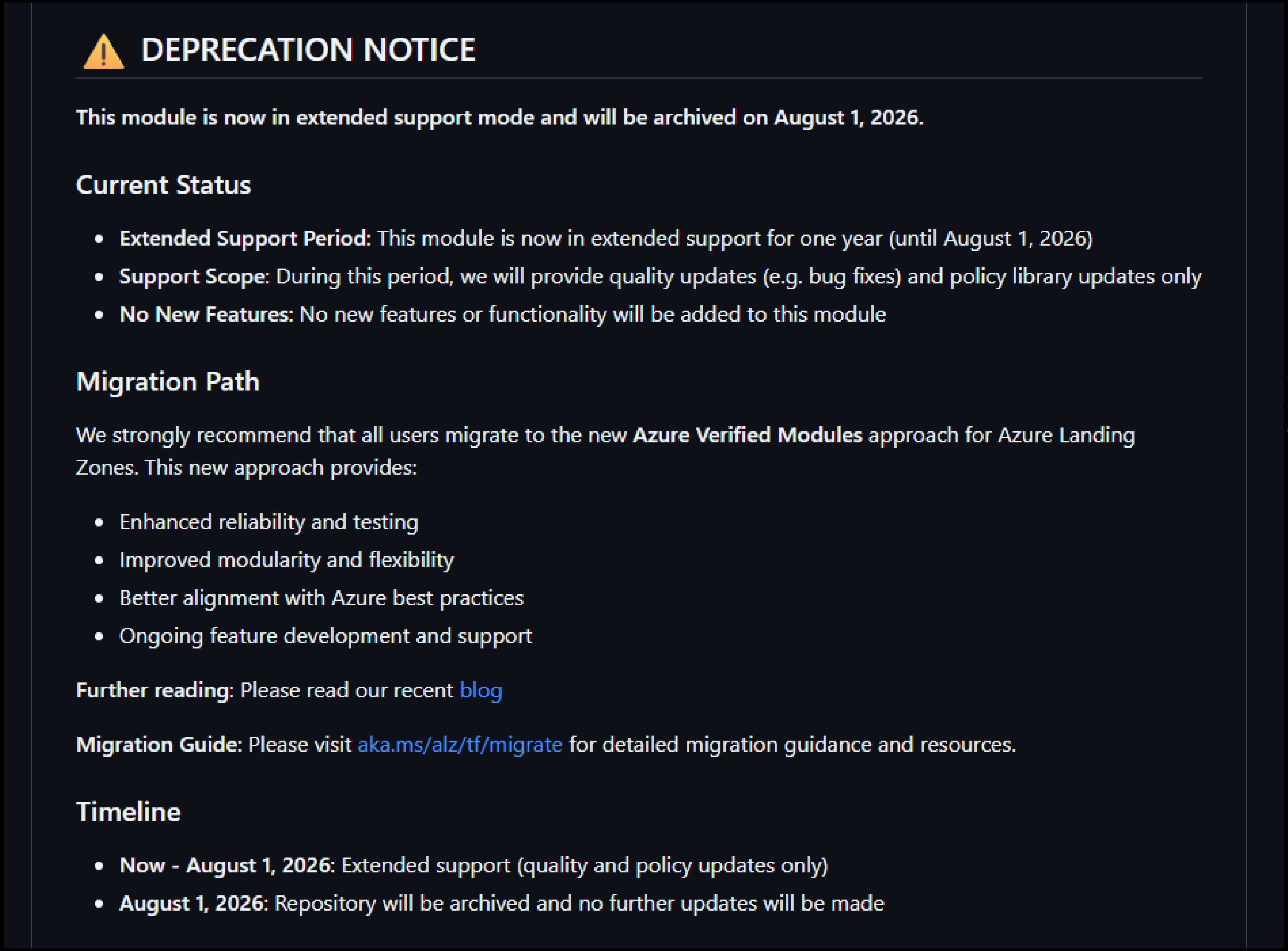
- Modular & Extensible Design: Flexible customization logic enables tailored and reusable deployments
- Strong Typing with UDTs: Safer, more consistent parameter validation through User Defined Types (UDTs)
- Network Flexibility: All networking properties available as defined in AVM — no longer restricted by hard-coded values
- Deployment Stacks Integration: Centralized lifecycle management, consistent clean-up, and streamlined lifecycle operations
- Native Bicep Advantages: Clean syntax, composable modules, built-in validation, etc.
- Preview Module: avm/ptn/alz/empty — foundation for ALZ accelerator pattern development ("Max" Test Case)

Demo



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

caf-enterprise-scale module deprecation 💤 🛌



⚠️ DEPRECATION NOTICE

This module is now in extended support mode and will be archived on August 1, 2026.

Current Status

- **Extended Support Period:** This module is now in extended support for one year (until August 1, 2026)
- **Support Scope:** During this period, we will provide quality updates (e.g. bug fixes) and policy library updates only
- **No New Features:** No new features or functionality will be added to this module

Migration Path

We strongly recommend that all users migrate to the new **Azure Verified Modules** approach for Azure Landing Zones. This new approach provides:

- Enhanced reliability and testing
- Improved modularity and flexibility
- Better alignment with Azure best practices
- Ongoing feature development and support

Further reading: Please read our recent blog

Migration Guide: Please visit aka.ms/alz/tf/migrate for detailed migration guidance and resources.

Timeline

- **Now - August 1, 2026:** Extended support (quality and policy updates only)
- **August 1, 2026:** Repository will be archived and no further updates will be made

Terraform State Importer Tool

A generic golang tool that can help with importing Terraform state for any Azure (azurerm or azapi) based Terraform Module, including AVM

- Guides you through the process of mapping resources and attributes
- Generates `import` blocks

- **Guidance for caf-enterprise-scale users (Azure Landing Zones): aka.ms/alz/tf/migrate**
- Tool: aka.ms/tf/migrate/tool

Terraform State Importer Tool

Stage 1 – Setup

- Target subscriptions and / or management groups
- KQL queries
- Exclusions
- Custom mappings where name alone is not sufficient
- Create the Target Terraform Module

Stage 2 – Resource Mapping

- Run the tool
- Examine the issues.csv
- Fix resource names in the target Terraform module
- Repeat ⟳

- For any unmatched resources decide:
  - Ignore
  - Delete
  - Delete / Recreate
- Save resolved-issues.csv

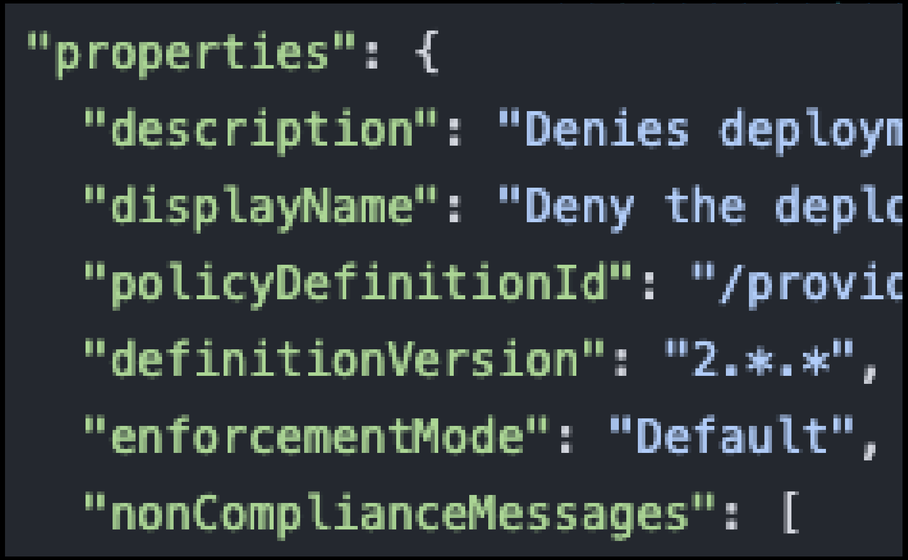
Stage 3 – Attribute Mapping

- Run the tool with the resolved-issues.csv
  - Generates import blocks
  - Generates 'delete' blocks
- Examine the filtered plan file
- Update any attributes of resources that need to match prior settings
- Repeat ⟳

Run: `terraform apply`

Policy Versioning (built-in)

- The ALZ provider now understands policy versions and fetches all built-in versions from Azure
- You can specify a wildcard in your version property of your assignment (or policy set)
- You MUST allow wildcard for PATCH versions, e.g. 1.0.*
- Versions:
  - Provider: v0.20.0
  - Module: v0.14.0



```
"properties": {
  "description": "Denies deploym
  "displayName": "Deny the deplo
  "policyDefinitionId": "/provi
  "definitionVersion": "2.*.*",
  "enforcementMode": "Default",
  "nonComplianceMessages": [
```

Other things

Schema validation toggle

Can change API versions

Random UUIDs for role assignment names

User-Assigned Managed Identity now working for policies*

Minimum Terraform version of 1.12

Experimental OpenTofu support for 1.10

Module Consolidation and Explicit Variables

Child modules merged into submodules and deprecated

- avm-ptn-alz-connectivity-hub-and-spoke-vnet
  - 🗑️ avm-ptn-hubnetworking
  - 🗑️ avm-ptn-vnetgateway

- avm-ptn-alz-connectivity-virtual-wan
  - 🗑️ avm-ptn-virtualwan

Module Consolidation and Explicit Variables

Connectivity modules now have comprehensive explicit variable declarations

- avm-ptn-alz-connectivity-hub-and-spoke-vnet
- avm-ptn-alz-connectivity-virtual-wan

- Some variables have been de-nested
- More options have been added
- All Virtual WAN options exposed in the main variable
- Enabled flags move up a layer and grouped together

Module Consolidation and Explicit Variables

Connectivity modules now have simpler interface

- avm-ptn-alz-connectivity-hub-and-spoke-vnet
- avm-ptn-alz-connectivity-virtual-wan

- IP ranges auto calculated if not supplied
- Availability zones looked up and set automatically
- Resource names templated and set automatically

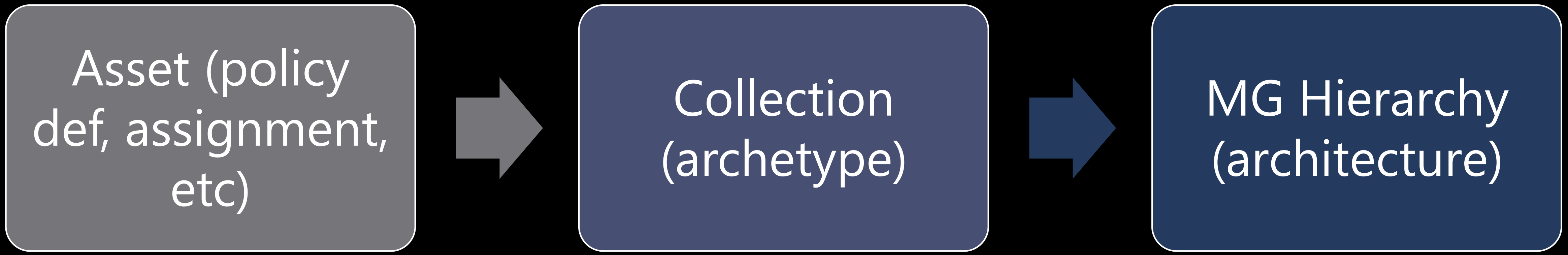
```
module "platform_landing_zone_connectivity" {
  source  = "Azure/avm-ptn-alz-connectivity-hub-and-spoke-vnet/azurerm"
  version = "0.14.6"
  hub_virtual_networks = {
    primary = {
      location          = "uksouth"
      default_parent_id = "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rg-hub-uksouth-001"
    }
    secondary = {
      location          = "ukwest"
      default_parent_id = "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rg-hub-uksouth-001"
    }
  }
}
```

ALZ Library Overview & Deep Dive

Why and What

- Separation of business logic and data (module + policies)
- Hosted at `Azure/Azure-Landing-Zones-Library` on GitHub
- Library members inside `platform/` directory
- Tagging in the form of `platform/member@YYYY.MM.P`
- Docs: Azure Landing Zones Library Documentation

Library resources



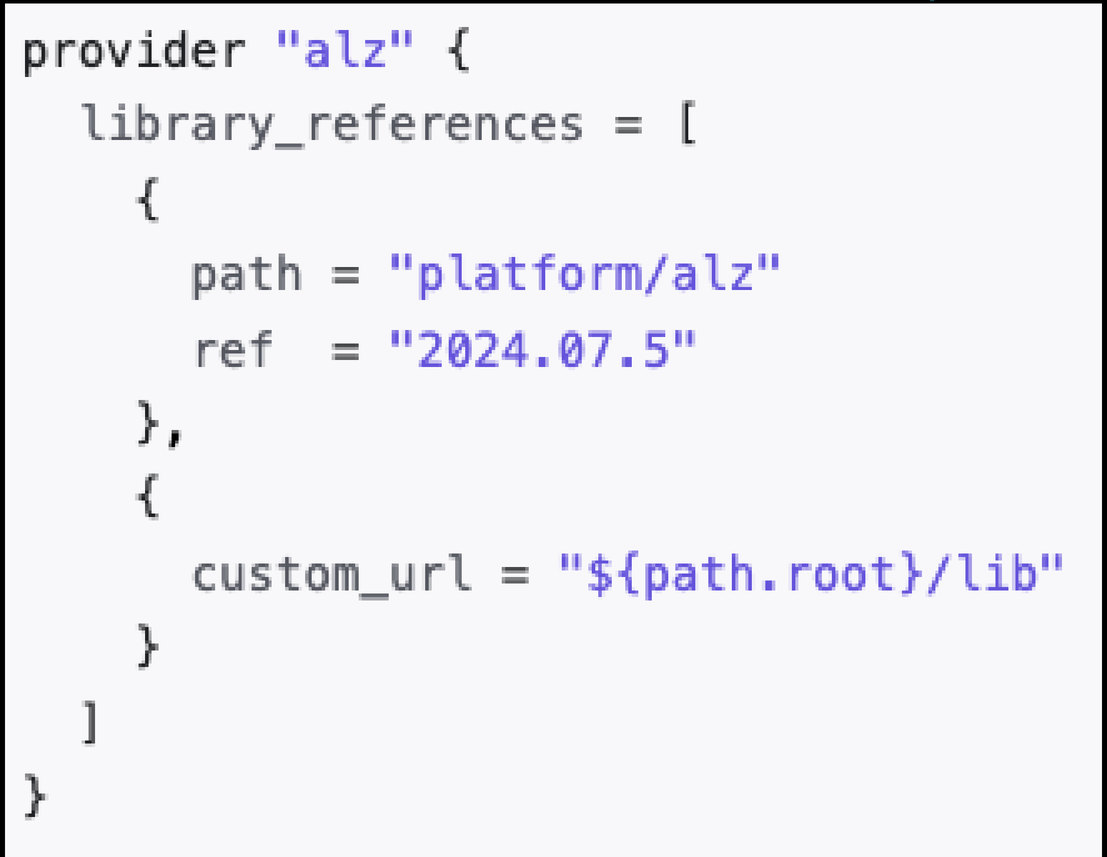
Asset (policy def, assignment, etc)

Collection (archetype)

MG Hierarchy (architecture)

Library references

- Specified as provider configuration
- Two types:
  - Azure-Landing-Zones-Library path and reference (git tag)
  - Custom URL or local path
- Processed in order! So put dependent libraries first
- Implicit dependencies
  - alz_library_metadata.json can contain dependencies, which are processed first



```
provider "alz" {
  library_references = [
    {
      path = "platform/alz"
      ref  = "2024.07.5"
    },
    {
      custom_url = "${path.root}/lib"
    }
  ]
}
```

This is the same

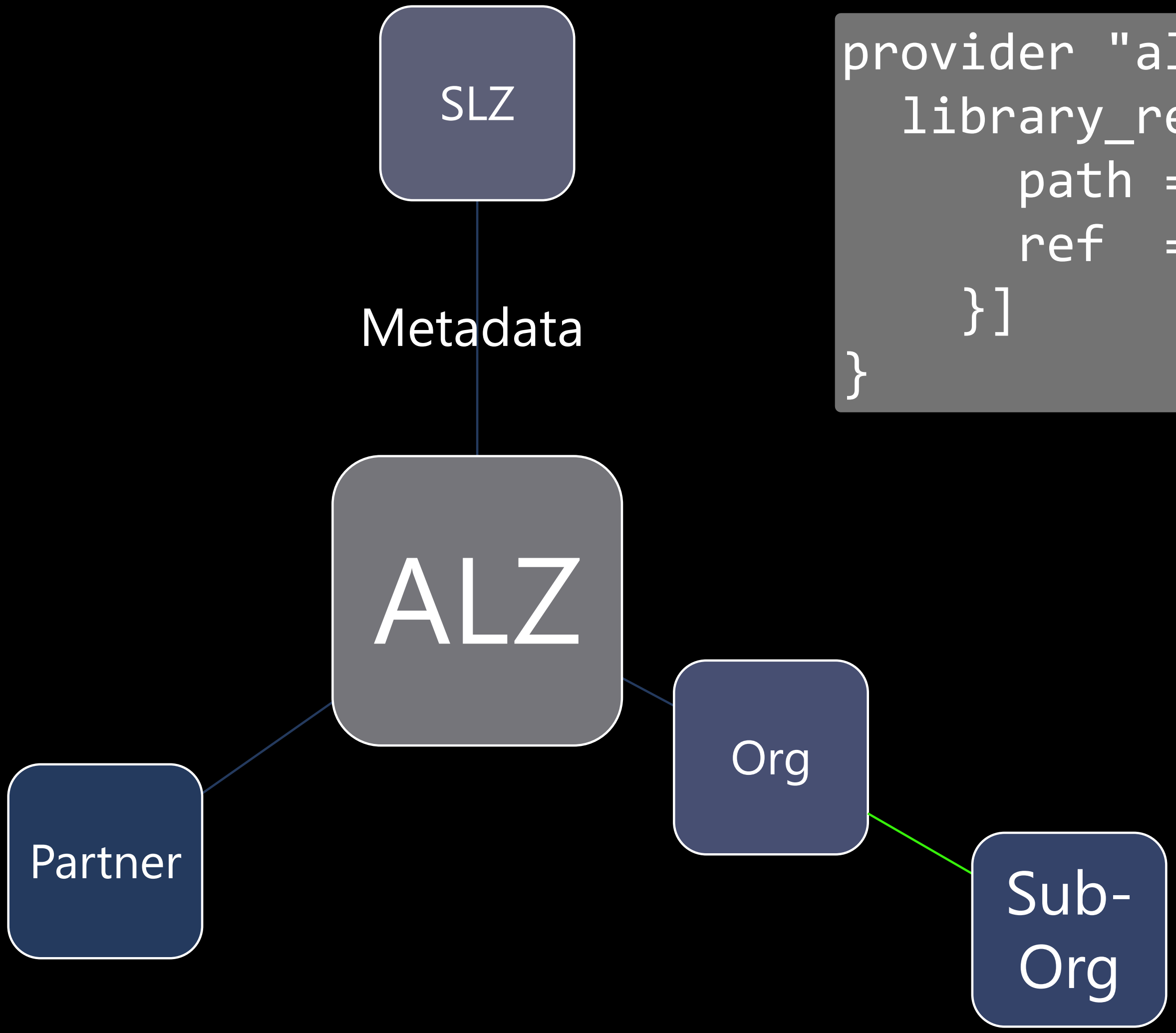
```
provider "alz" {
  library_references = [
    {
      path = "platform/alz"
      ref  = "2025.09.3"
    },
    {
      custom_url = "${path.root}/lib"
    }
  ]
}
```

```
provider "alz" {
  library_references =  {
      custom_url = "${path.root}/lib"
    }]
}
```

+

```
📂
 - 📂 lib
   - alz_library_metadata.json
```

Composition



```
provider "alz" {
  library_references = [{
      path = "platform/slz"
      ref  = "2025.09.0"
    }]
}
```

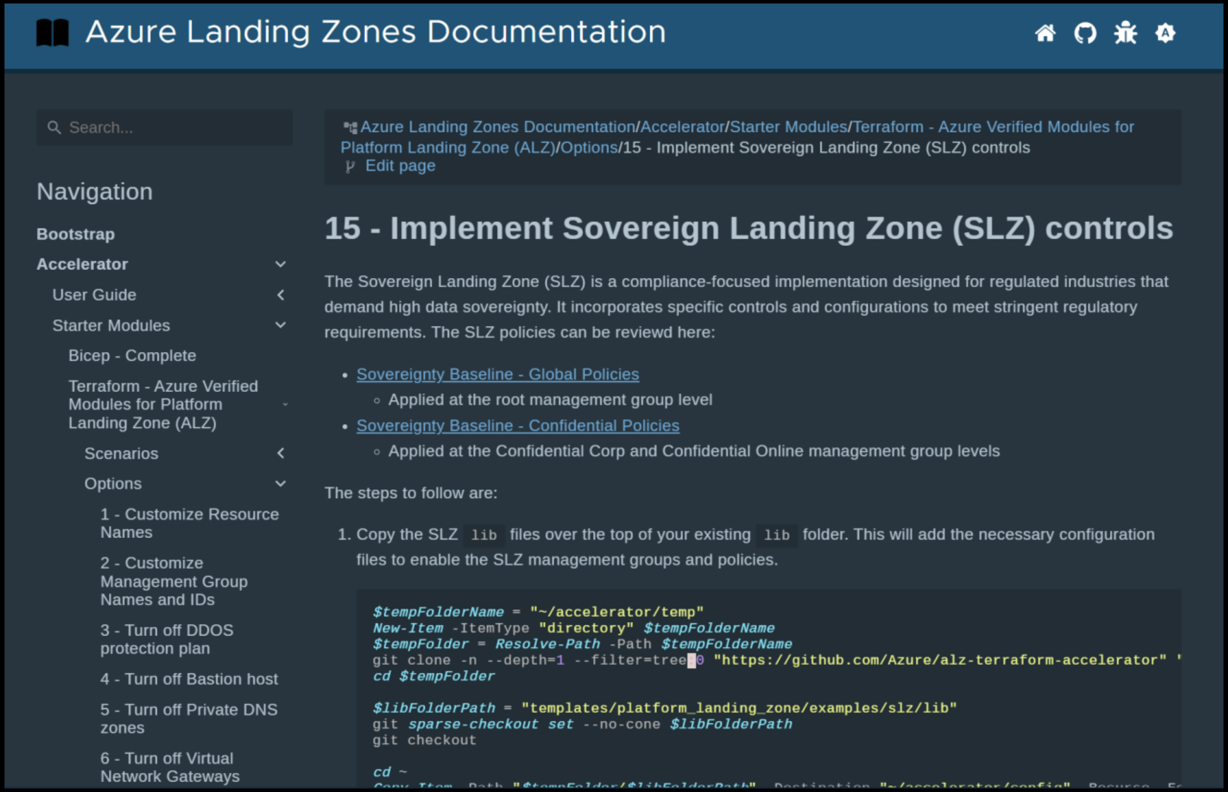
ALZ IaC Accelerator Updates

Security Management Group

- Separate management group and subscription for Sentinel
- Added to Bicep and Terraform Accelerators

Terraform Sovereign landing zone option

- Existing separate starter module deprecated
- Updates to the SLZ library
- Addition of new option and pre-templated lib files


Azure Landing Zones Documentation
Search...
Navigation
Bootstrap
Accelerator
User Guide
Starter Modules
Bicep - Complete
Terraform - Azure Verified Modules for Platform Landing Zone (ALZ)
Scenarios
Options
1 - Customize Resource Names
2 - Customize Management Group Names and IDs
3 - Turn off DDOS protection plan
4 - Turn off Bastion host
5 - Turn off Private DNS zones
6 - Turn off Virtual Network Gateways

Azure Landing Zones Documentation/Accelerator/Starter Modules/Terraform - Azure Verified Modules for Platform Landing Zone (ALZ)/Options/15 - Implement Sovereign Landing Zone (SLZ) controls

Edit page

15 - Implement Sovereign Landing Zone (SLZ) controls

The Sovereign Landing Zone (SLZ) is a compliance-focused implementation designed for regulated industries that demand high data sovereignty. It incorporates specific controls and configurations to meet stringent regulatory requirements. The SLZ policies can be reviewd here:

- Sovereignty Baseline - Global Policies
  - Applied at the root management group level
- Sovereignty Baseline - Confidential Policies
  - Applied at the Confidential Corp and Confidential Online management group levels

The steps to follow are:

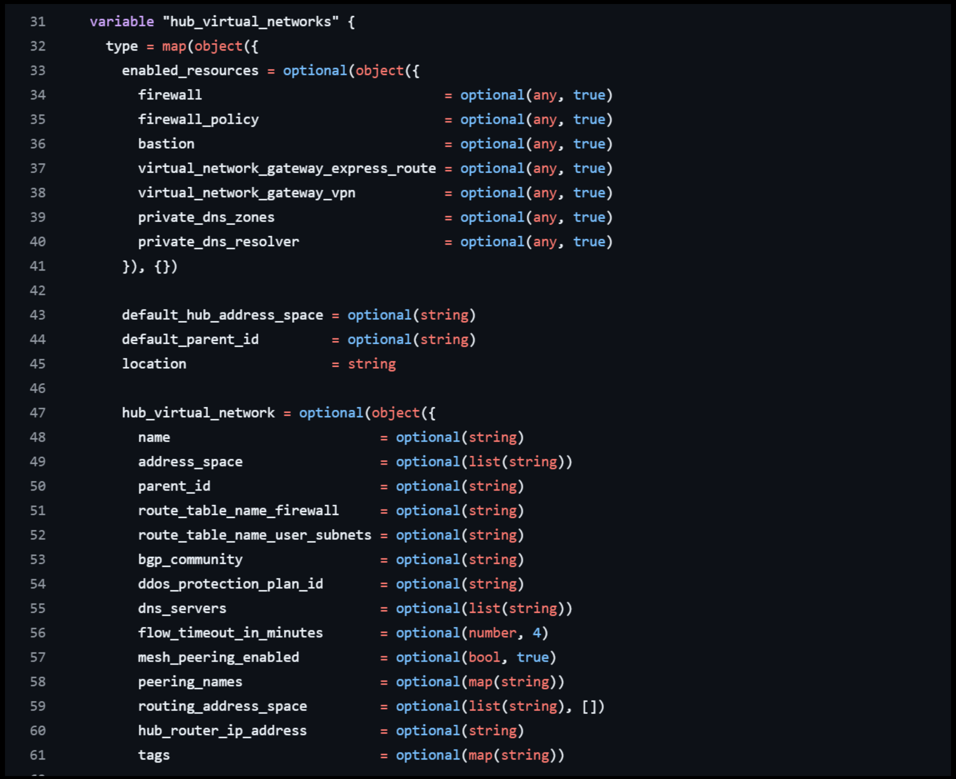
1. Copy the SLZ `lib` files over the top of your existing `lib` folder. This will add the necessary configuration files to enable the SLZ management groups and policies.

```
$tempFolderName = "~/accelerator/temp"
New-Item -ItemType "directory" $tempFolderName
$tempFolder = Resolve-Path -Path $tempFolderName
git clone -n --depth=1 --filter=tree:0 "https://github.com/Azure/alz-terraform-accelerator" '
cd $tempFolder

$libFolderPath = "templates/platform_landing_zone/examples/slz/lib"
git sparse-checkout set --no-cone $libFolderPath
git checkout

cd ~
Copy-Item -Path "$tempFolder/$libFolderPath" -Destination "~/accelerator/config" -Recurse -Fo
```

Terraform Explicit Variables

Accelerator starter module updated with explicit variables

- alz-terraform-accelerator



```
variable "hub_virtual_networks" {
  type = map(object({
    enabled_resources = optional(object({
      firewall                              = optional(any, true)
      firewall_policy                       = optional(any, true)
      bastion                               = optional(any, true)
      virtual_network_gateway_express_route = optional(any, true)
      virtual_network_gateway_vpn           = optional(any, true)
      private_dns_zones                     = optional(any, true)
      private_dns_resolver                  = optional(any, true)
    }), {})

    default_hub_address_space = optional(string)
    default_parent_id         = optional(string)
    location                  = string

    hub_virtual_network = optional(object({
      name                          = optional(string)
      address_space                 = optional(list(string))
      parent_id                     = optional(string)
      route_table_name_firewall     = optional(string)
      route_table_name_user_subnets = optional(string)
      bgp_community                 = optional(string)
      ddos_protection_plan_id       = optional(string)
      dns_servers                   = optional(list(string))
      flow_timeout_in_minutes       = optional(number, 4)
      mesh_peering_enabled          = optional(bool, true)
      peering_names                 = optional(map(string))
      routing_address_space         = optional(list(string), [])
      hub_router_ip_address         = optional(string)
      tags                          = optional(map(string))
```

Portal & Policy Refresh
H1 FY26 Updates

ALZ Portal News

aka.ms/alz/portal

- Security MG and Sub
  - *NEW* Security subscription required for full deployment

COMING SOON

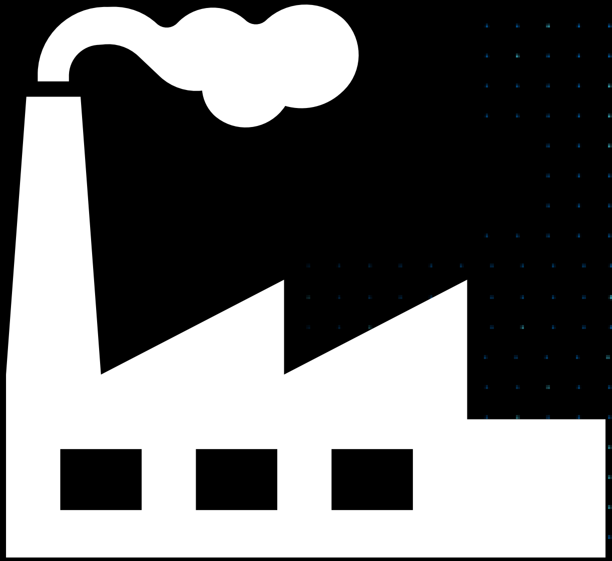
- Networking
  - Add support for Azure Bastion for all network topologies
  - Add support for Azure Private DNS Resolver for all network topologies (needs last mile config)
  - Added VWAN provisioning of sidecar network (needed for Bastion & Private DNS)
  - All Firewall SKUs now deploy with management NIC in the AzureFirewallManagementSubnet
- Standardizing resource group naming (CAF aligned)
- Remove support of non-public regions

ALZ Policy News

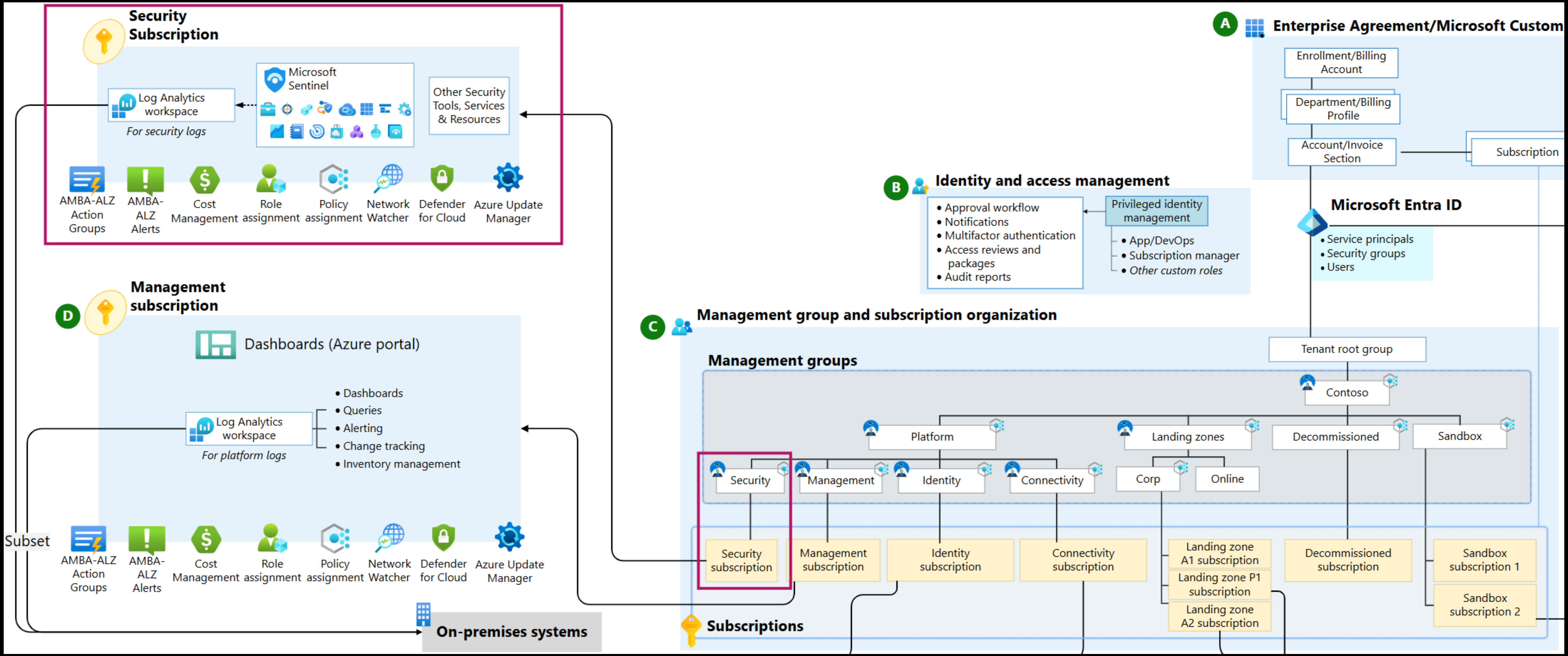
aka.ms/alz/whatsnew

- Policy Refresh H1 FY26 (In Progress)
  - Changing to 6 month release due to limited changes/resources
  - Community driving updates – keep the requests coming
- General updates
  - Defender (ASC) Contacts policy updated to support new attack path option (Critical)
  - Guardrails-SQL – added SQL/MI policy to enforce Entra ID only auth
  - Updated the optional FileServices-InsecureSmb policies to support Files deployed with maximum compatibility
  - Quality workflow updates

ALZ MS Learn & Other Updates



Security Subscription & Management Group added



Security Subscription

Log Analytics workspace

For security logs

Microsoft Sentinel

Other Security Tools, Services & Resources

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

D **Management subscription**

Dashboards (Azure portal)

Log Analytics workspace

For platform logs

- Dashboards
- Queries
- Alerting
- Change tracking
- Inventory management

Subset

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

On-premises systems

A **Enterprise Agreement/Microsoft Custom**

Enrollment/Billing Account

Department/Billing Profile

Account/Invoice Section

Subscription

B **Identity and access management**

- Approval workflow
- Notifications
- Multifactor authentication
- Access reviews and packages
- Audit reports

Privileged identity management

- App/DevOps
- Subscription manager
- *Other custom roles*

Microsoft Entra ID

- Service principals
- Security groups
- Users

C **Management group and subscription organization**

Management groups

Tenant root group

Contoso

Platform · Landing zones · Decommissioned · Sandbox

Security · Management · Identity · Connectivity · Corp · Online

Subscriptions

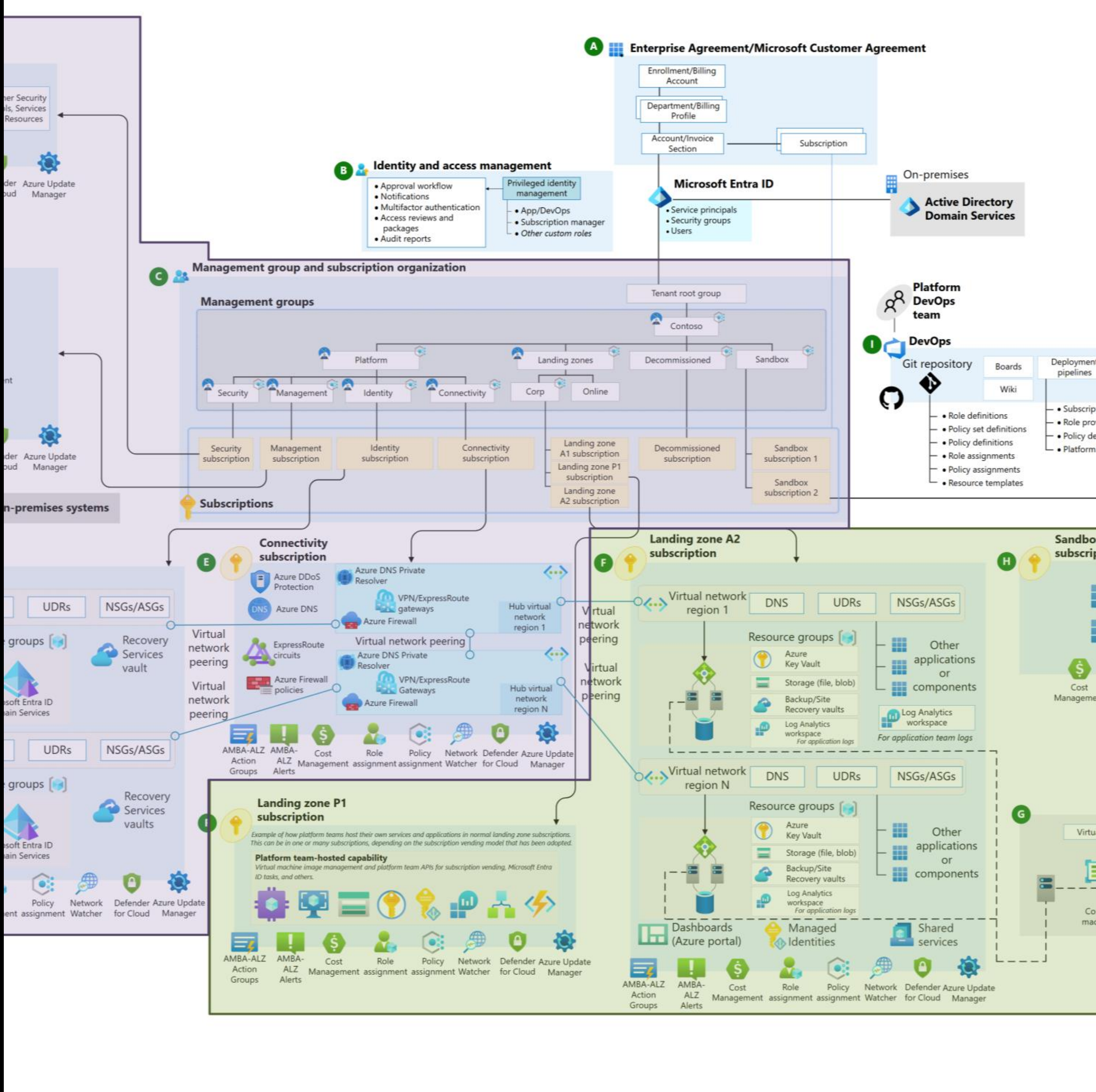
Security subscription · Management subscription · Identity subscription · Connectivity subscription · Landing zone A1 subscription · Landing zone P1 subscription · Landing zone A2 subscription · Decommissioned subscription · Sandbox subscription 1 · Sandbox subscription 2

Learn more

Platform vs Application Clarity

"An Azure landing zone consists of one platform landing zone and one or more application landing zones. It's worth explaining the function of both in more detail."

Learn more



Terminology to use going forward

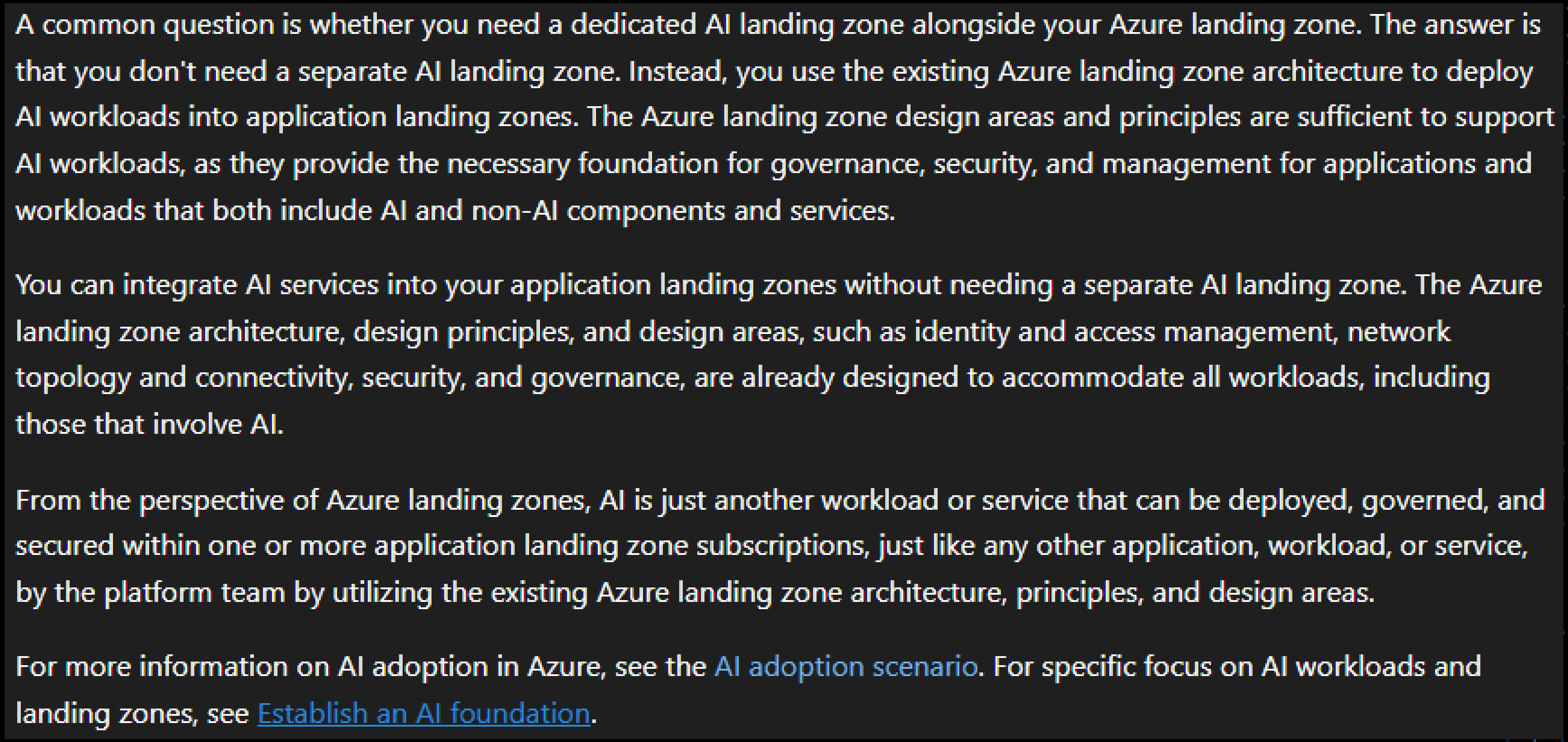
Platform landing zone (singular)

- Management Groups & Policies
- Resource organization
- Shared services subscriptions (management, connectivity, security, identity)

Application landing zones (plural)

- Where application teams deploy, host and run their workloads and services
- Inherit Azure Policies from Management Group hierarchy
- Utilize shared services subscriptions

AI in Azure landing zones clarity 🔥



A common question is whether you need a dedicated AI landing zone alongside your Azure landing zone. The answer is that you don't need a separate AI landing zone. Instead, you use the existing Azure landing zone architecture to deploy AI workloads into application landing zones. The Azure landing zone design areas and principles are sufficient to support AI workloads, as they provide the necessary foundation for governance, security, and management for applications and workloads that both include AI and non-AI components and services.

You can integrate AI services into your application landing zones without needing a separate AI landing zone. The Azure landing zone architecture, design principles, and design areas, such as identity and access management, network topology and connectivity, security, and governance, are already designed to accommodate all workloads, including those that involve AI.

From the perspective of Azure landing zones, AI is just another workload or service that can be deployed, governed, and secured within one or more application landing zone subscriptions, just like any other application, workload, or service, by the platform team by utilizing the existing Azure landing zone architecture, principles, and design areas.

For more information on AI adoption in Azure, see the AI adoption scenario. For specific focus on AI workloads and landing zones, see Establish an AI foundation.

Learn more

Azure Landing Zone Design Principles | Refreshed

- Enable Autonomy for Innovation and Transformation
- Security and Compliance By-Default
- Governance At-Scale with Sustainable Cloud Engineering

Learn more

Subscription Democratization

Policy Driven Governance

Single Control and Management Plane

Application Centric and Archetype-Neutral

Azure Native Design and Platform Roadmap Alignment

What we are/have been working on…

Product & Service Updates ♻️

- AVNM
- Service Groups
- Default outbound access
- Private DNS Resolver
- Multi-Region Private DNS Zones Guidance
- Much more…

ALZ Bicep -> Azure Verified Modules for Platform Landing Zones (ALZ) – Bicep 💪

Security Management Group 🔒

Policy updates & versioning 📃

GitHub Issue Management & Consolidation ❗

Simplifying the ALZ Accelerator 🧮

Retire the ALZ Portal Accelerator 👀 😳

Microsoft Sovereign Cloud & SLZ 👑

Microsoft Defender for Cloud integrated in Sub Vending modules 🛡️

NAT Gateway integrated into Sub Vending modules 🌐

Sovereign landing zone

Sovereign landing zone (SLZ)

The platform landing zone - built on Azure landing zone (ALZ)- empowering organizations to enforce sovereignty controls in the public cloud

Variant of Azure landing zone (ALZ)

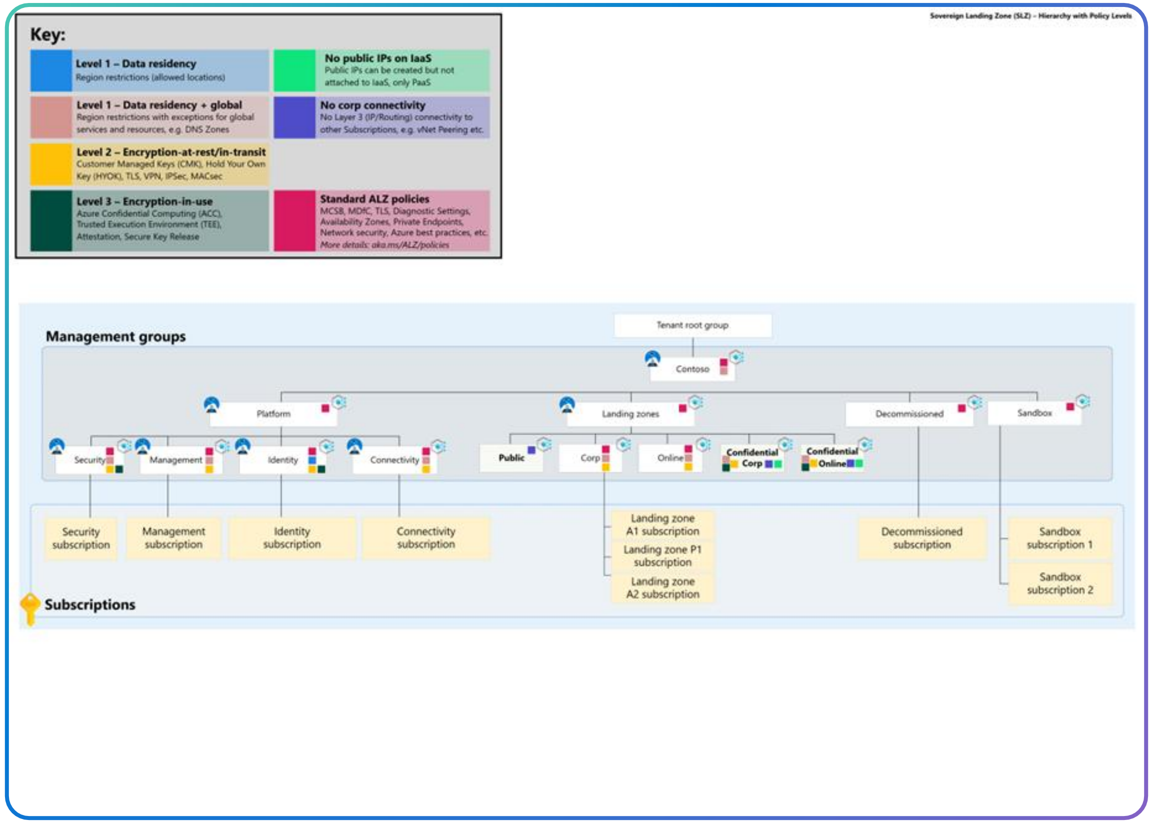
- Builds on top of already well-established ALZ architecture, guidance, tooling, and best-practices.
- Expands Management Group hierarchy to support sovereign requirements – following tailoring guidance.
- Allows existing ALZ consumers to adopt SLZ easily with existing tooling without having to restart from scratch.

Accelerates enforcing Level 1, 2, & 3 controls

- Provides Microsoft maintained Azure Policy definitions, initiatives, and default assignments upon the Management Group hierarchy to enforce sovereign controls
- Provides guidance on Azure Key Vault Managed HSM placement in architecture

Sovereign landing zone is **available now**
**Terraform only today. Bicep in development*

Learn more

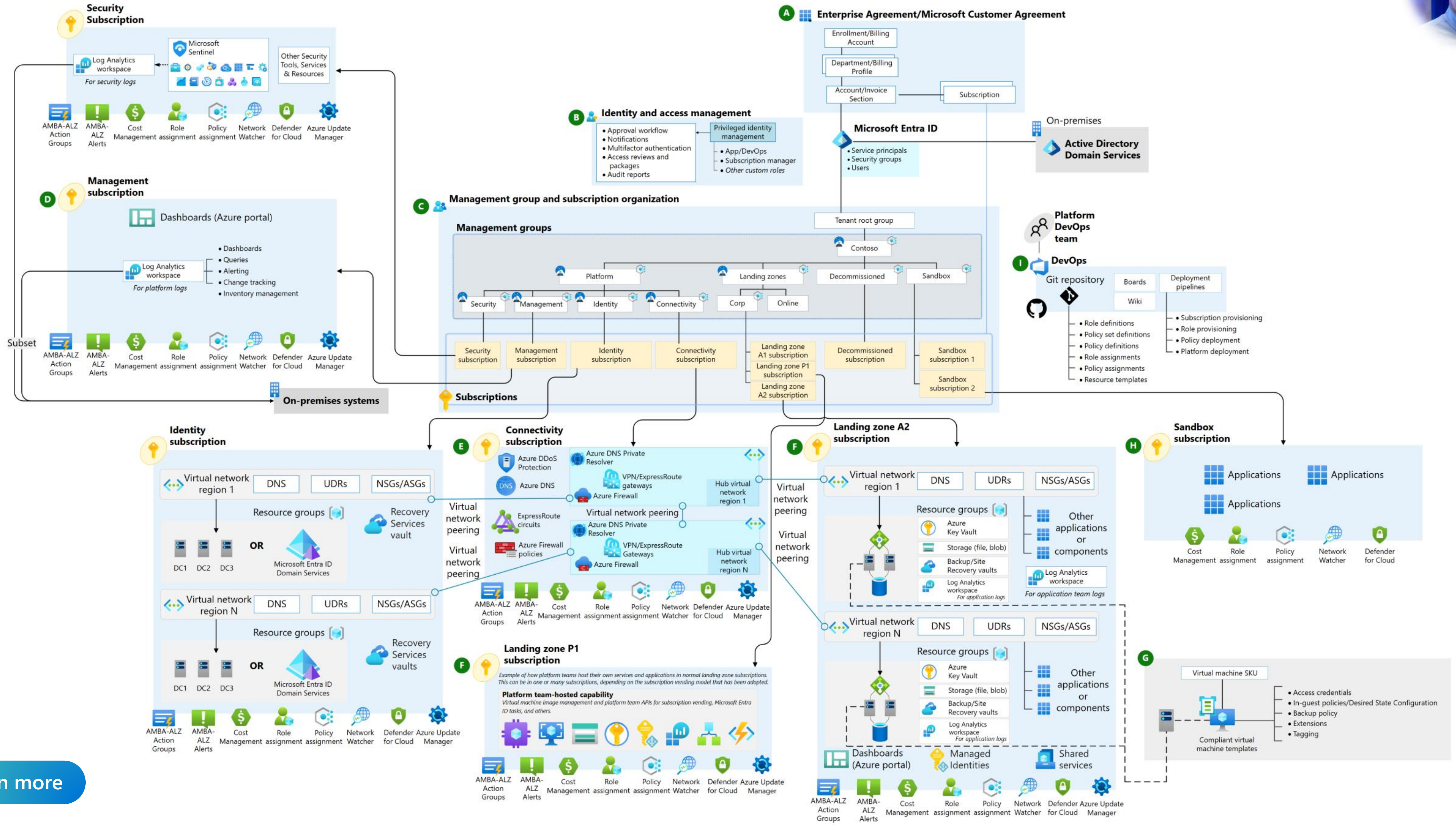

Sovereign Landing Zone (SLZ) – Hierarchy with Policy Levels

Key:

- **Level 1 – Data residency** Region restrictions (allowed locations)
- **Level 1 – Data residency + global** Region restrictions with exceptions for global services and resources, e.g. DNS Zones
- **Level 2 – Encryption-at-rest/in-transit** Customer Managed Keys (CMK), Hold Your Own Key (HYOK), TLS, VPN, IPSec, MACsec
- **Level 3 – Encryption-in-use** Azure Confidential Computing (ACC), Trusted Execution Environment (TEE), Attestation, Secure Key Release
- **No public IPs on IaaS** Public IPs can be created but not attached to IaaS, only PaaS
- **No corp connectivity** No Layer 3 (IP/Routing) connectivity to other Subscriptions, e.g. vNet Peering etc.
- **Standard ALZ policies** MCSB, MDfC, TLS, Diagnostic Settings, Availability Zones, Private Endpoints, Network security, Azure best practices, etc. *More details: aka.ms/ALZ/policies*

Classified as Microsoft Confidential

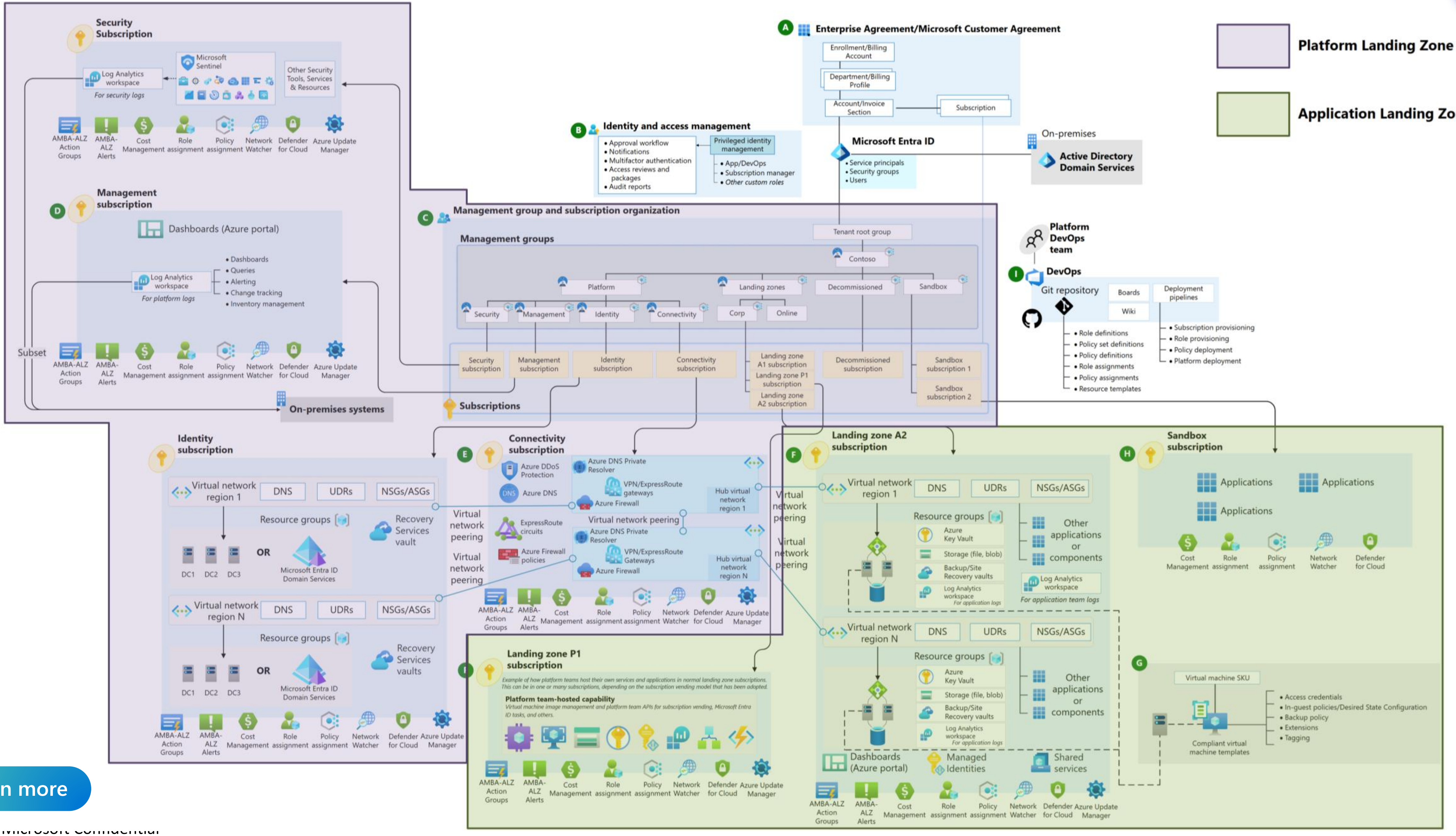
First, a refresh on the Azure landing zone architecture



Learn more

Classified

Platform vs Application landing zones

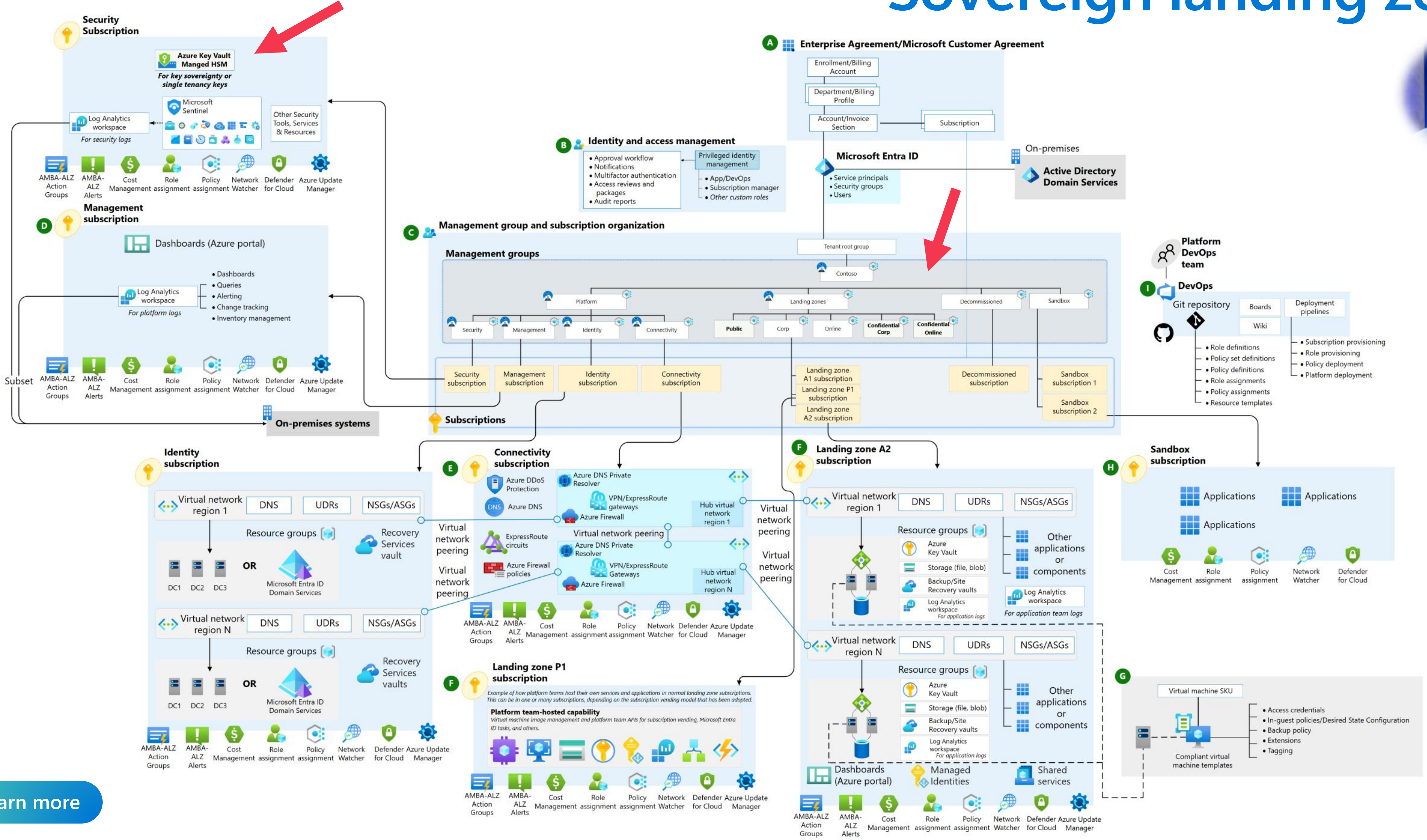


▨ Platform Landing Zone

▨ Application Landing Zones

Learn more

Sovereign landing zone



Security Subscription

Azure Key Vault Manged HSM

For key sovereignty or single tenancy keys

Log Analytics workspace

For security logs

Microsoft Sentinel

Other Security Tools, Services & Resources

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

D Management subscription

Dashboards (Azure portal)

Log Analytics workspace

For platform logs

- Dashboards
- Queries
- Alerting
- Change tracking
- Inventory management

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

Subset

On-premises systems

A Enterprise Agreement/Microsoft Customer Agreement

Enrollment/Billing Account

Department/Billing Profile

Account/Invoice Section

Subscription

B Identity and access management

- Approval workflow
- Notifications
- Multifactor authentication
- Access reviews and packages
- Audit reports

Privileged identity management

- App/DevOps
- Subscription manager
- *Other custom roles*

Microsoft Entra ID

- Service principals
- Security groups
- Users

On-premises

Active Directory Domain Services

C Management group and subscription organization

Tenant root group

Management groups

Contoso

Platform · Landing zones · Decommissioned · Sandbox

Security · Management · Identity · Connectivity

Public · Corp · Online · Confidential Corp · Confidential Online

Subscriptions

Security subscription · Management subscription · Identity subscription · Connectivity subscription

Landing zone A1 subscription · Landing zone P1 subscription · Landing zone A2 subscription

Decommissioned subscription

Sandbox subscription 1 · Sandbox subscription 2

Platform DevOps team

I DevOps

Git repository · Boards · Wiki · Deployment pipelines

- Role definitions
- Policy set definitions
- Policy definitions
- Role assignments
- Policy assignments
- Resource templates

- Subscription provisioning
- Role provisioning
- Policy deployment
- Platform deployment

Identity subscription

Virtual network region 1 · DNS · UDRs · NSGs/ASGs

Resource groups

DC1 · DC2 · DC3 · OR · Microsoft Entra ID Domain Services

Recovery Services vault

Virtual network region N · DNS · UDRs · NSGs/ASGs

Resource groups

DC1 · DC2 · DC3 · OR · Microsoft Entra ID Domain Services

Recovery Services vaults

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

E Connectivity subscription

Azure DDoS Protection

Azure DNS

ExpressRoute circuits

Azure Firewall policies

Azure DNS Private Resolver · VPN/ExpressRoute gateways · Azure Firewall · Hub virtual network region 1

Virtual network peering

Azure DNS Private Resolver · VPN/ExpressRoute Gateways · Azure Firewall · Hub virtual network region N

Virtual network peering

Virtual network peering

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

F Landing zone P1 subscription

Example of how platform teams host their own services and applications in normal landing zone subscriptions. This can be in one or many subscriptions, depending on the subscription vending model that has been adopted.

Platform team-hosted capability

Virtual machine image management and platform team APIs for subscription vending, Microsoft Entra ID tasks, and others.

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

F Landing zone A2 subscription

Virtual network peering

Virtual network peering

Virtual network region 1 · DNS · UDRs · NSGs/ASGs

Resource groups

Azure Key Vault · Storage (file, blob) · Backup/Site Recovery vaults · Log Analytics workspace *For application logs*

Other applications or components

Log Analytics workspace

For application team logs

Virtual network region N · DNS · UDRs · NSGs/ASGs

Resource groups

Azure Key Vault · Storage (file, blob) · Backup/Site Recovery vaults · Log Analytics workspace *For application logs*

Other applications or components

Dashboards (Azure portal) · Managed Identities · Shared services

AMBA-ALZ Action Groups · AMBA-ALZ Alerts · Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud · Azure Update Manager

H Sandbox subscription

Applications · Applications · Applications

Cost Management · Role assignment · Policy assignment · Network Watcher · Defender for Cloud

G

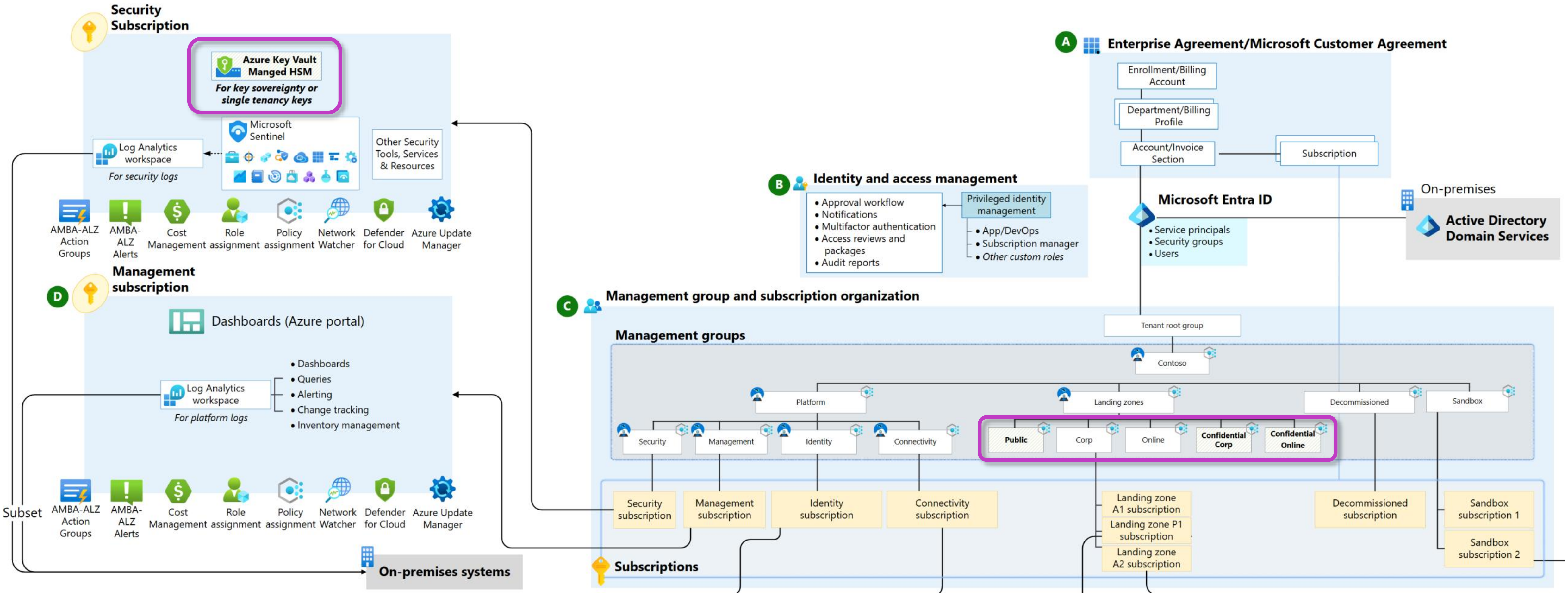
Virtual machine SKU

Compliant virtual machine templates

- Access credentials
- In-guest policies/Desired State Configuration
- Backup policy
- Extensions
- Tagging

Learn more

Sovereign landing zone differences from ALZ



Security Subscription

Azure Key Vault Manged HSM

For key sovereignty or single tenancy keys

Microsoft Sentinel

Log Analytics workspace

For security logs

Other Security Tools, Services & Resources

AMBA-ALZ Action Groups

AMBA-ALZ Alerts

Cost Management

Role assignment

Policy assignment

Network Watcher

Defender for Cloud

Azure Update Manager

D Management subscription

Dashboards (Azure portal)

Log Analytics workspace

For platform logs

- Dashboards
- Queries
- Alerting
- Change tracking
- Inventory management

AMBA-ALZ Action Groups

AMBA-ALZ Alerts

Cost Management

Role assignment

Policy assignment

Network Watcher

Defender for Cloud

Azure Update Manager

Subset

On-premises systems

A Enterprise Agreement/Microsoft Customer Agreement

Enrollment/Billing Account

Department/Billing Profile

Account/Invoice Section

Subscription

B Identity and access management

- Approval workflow
- Notifications
- Multifactor authentication
- Access reviews and packages
- Audit reports

Privileged identity management

- App/DevOps
- Subscription manager
- *Other custom roles*

Microsoft Entra ID

- Service principals
- Security groups
- Users

On-premises

Active Directory Domain Services

C Management group and subscription organization

Management groups

Tenant root group

Contoso

Platform

Landing zones

Decommissioned

Sandbox

Security

Management

Identity

Connectivity

Public

Corp

Online

Confidential Corp

Confidential Online

Security subscription

Management subscription

Identity subscription

Connectivity subscription

Landing zone A1 subscription

Landing zone P1 subscription

Landing zone A2 subscription

Decommissioned subscription

Sandbox subscription 1

Sandbox subscription 2

Subscriptions

Learn more

Policy Initiatives for L1, L2, & L3

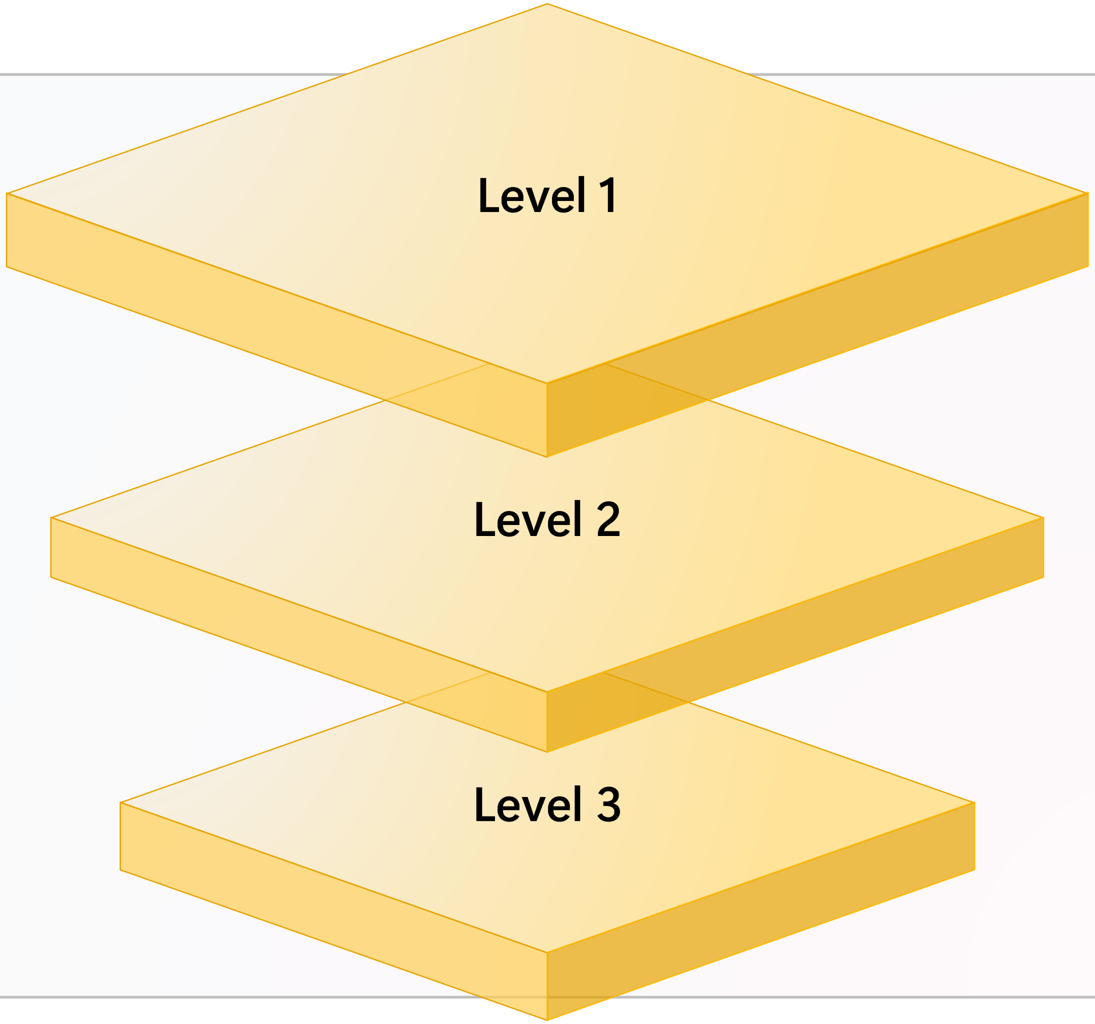
Azure Policy enforces controls across all levels

- **Level 1:** Residency checks and region restrictions.
- **Level 2:** TLS version enforcement, CMK enforcement, HSM enforcement.
- **Level 3:** Azure Confidential Computing policies.

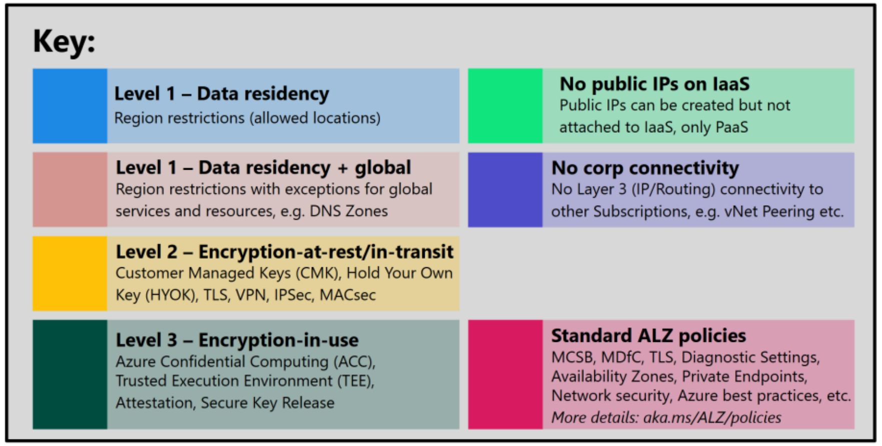
Combine these into policy initiatives for consistent governance.

Learn more about Controls & Principles in Sovereign Public Cloud

Learn how Sovereign landing zone implements these in Azure



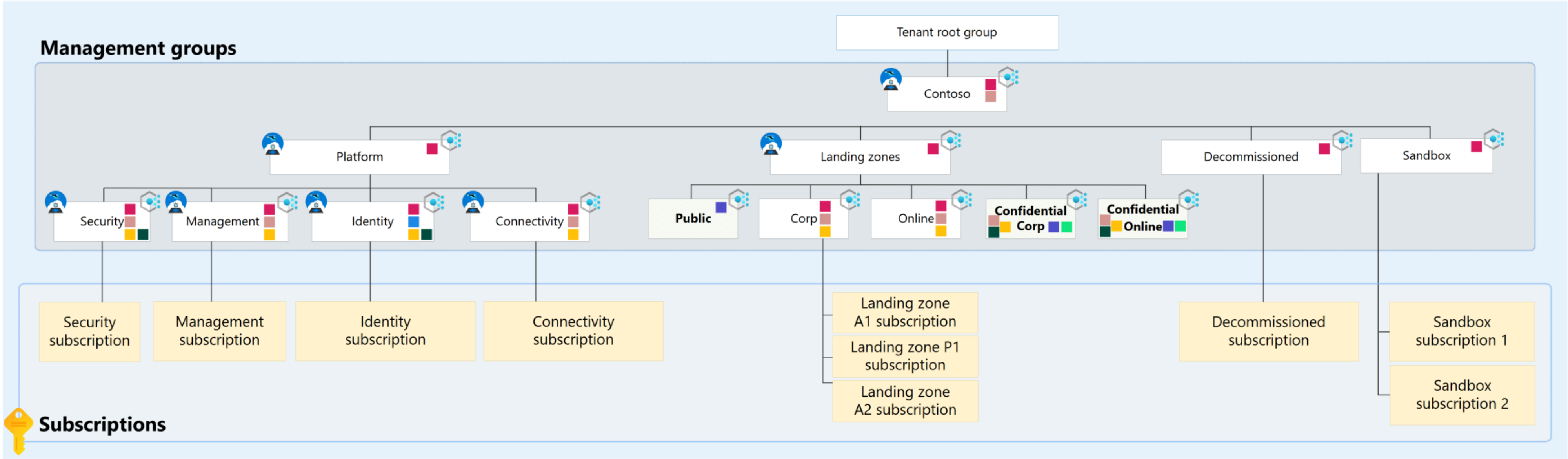
How SLZ accelerates L1, L2, & L3



Key:

🟦	**Level 1 – Data residency** Region restrictions (allowed locations)	🟩	**No public IPs on IaaS** Public IPs can be created but not attached to IaaS, only PaaS
🟫	**Level 1 – Data residency + global** Region restrictions with exceptions for global services and resources, e.g. DNS Zones	🟪	**No corp connectivity** No Layer 3 (IP/Routing) connectivity to other Subscriptions, e.g. vNet Peering etc.
🟨	**Level 2 – Encryption-at-rest/in-transit** Customer Managed Keys (CMK), Hold Your Own Key (HYOK), TLS, VPN, IPSec, MACsec		
⬛	**Level 3 – Encryption-in-use** Azure Confidential Computing (ACC), Trusted Execution Environment (TEE), Attestation, Secure Key Release	🟥	**Standard ALZ policies** MCSB, MDfC, TLS, Diagnostic Settings, Availability Zones, Private Endpoints, Network security, Azure best practices, etc. *More details: aka.ms/ALZ/policies*

- SLZ uses Azure Policy and management groups to enforce sovereign controls at scale.
- Workloads are classified to apply Level 1, 2, and 3 data protection controls.
- Policy initiatives ensure compliance for residency, encryption, and confidential computing.
- Architecture is flexible for tailoring policies to organizational data classifications.



Learn more

Classified as Microsoft Confidential

Microsoft Ignite

Join me at Microsoft Ignite in San Fransico!

November 17-21, 2025

Jack Tracey

Azure Landing Zone & Azure Verified Modules Technical Lead

AMBA-ALZ Updates

aka.ms/amba/alz

AMBA Updates

aka.ms/amba/alz/whatsnew

- New features and alerts:
  - Adoption of the ***new*** built-in Service Health alert policy
  - Adoption of the ***new*** least privileged “Monitoring Policy Contributor” built-in Azure role
  - Promoted the following alerts to GA:
    - Activity Log Route Table Delete Alert
    - Activity Log Routes Delete Alert
  - Official documentation guide for deploying AMBA-ALZ using Terraform

- New Connectivity initiative - Part #2 initiative including ***12 new*** alerts
- ***6*** bugs fixed
- Documentation improvements

AMBA Roadmap

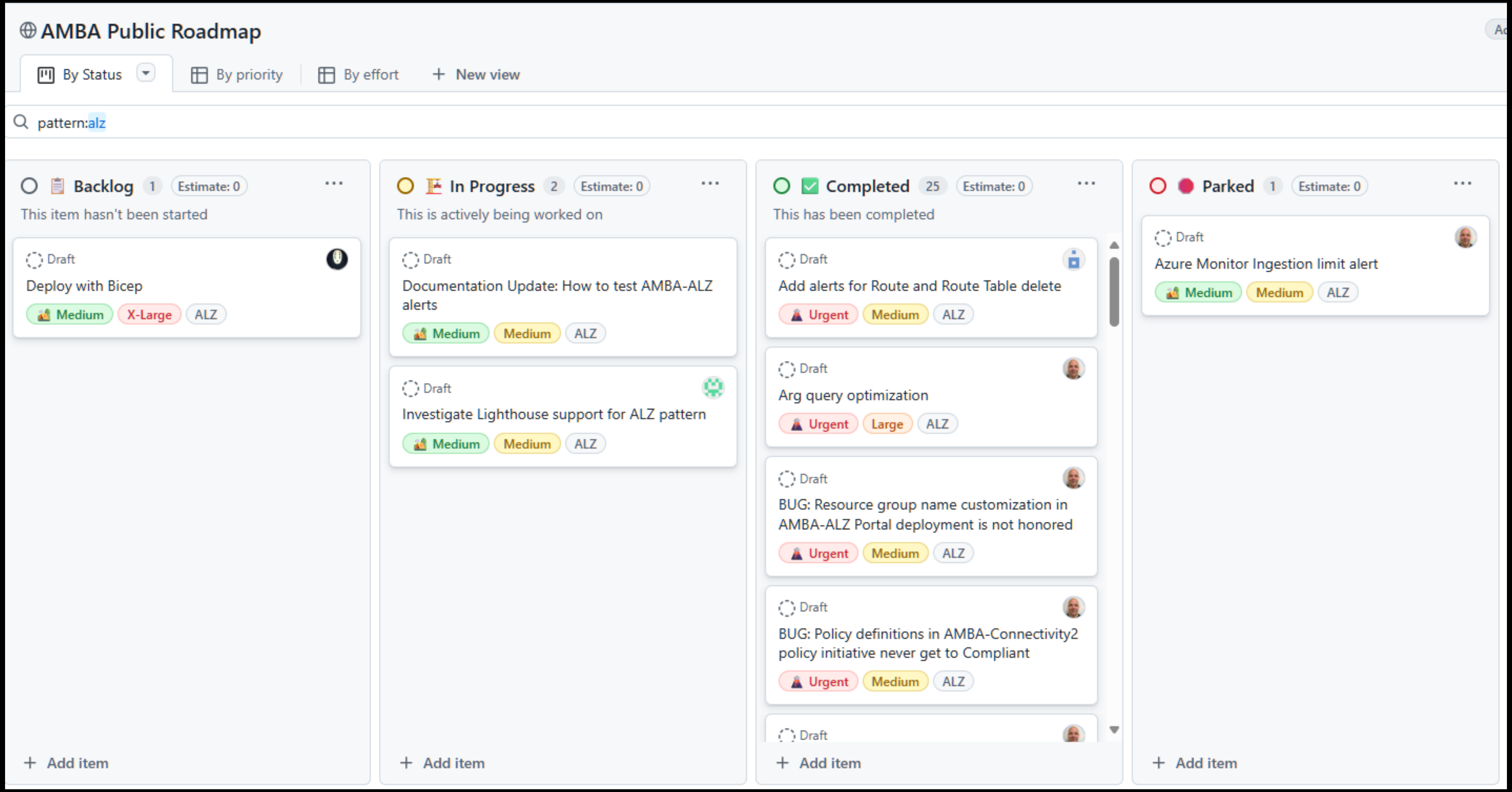
aka.ms/amba/roadmap/alz

- 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
- Investigating Lighthouse support for ALZ pattern

- 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

+ Add item

In Progress 2 Estimate: 0
This is actively being worked on

- Draft — Documentation Update: How to test AMBA-ALZ alerts — Medium · Medium · ALZ
- Draft — Investigate Lighthouse support for ALZ pattern — Medium · Medium · ALZ

+ Add item

Completed 25 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: Policy definitions in AMBA-Connectivity2 policy initiative never get to Compliant — Urgent · Medium · ALZ
- Draft

+ Add item

Parked 1 Estimate: 0

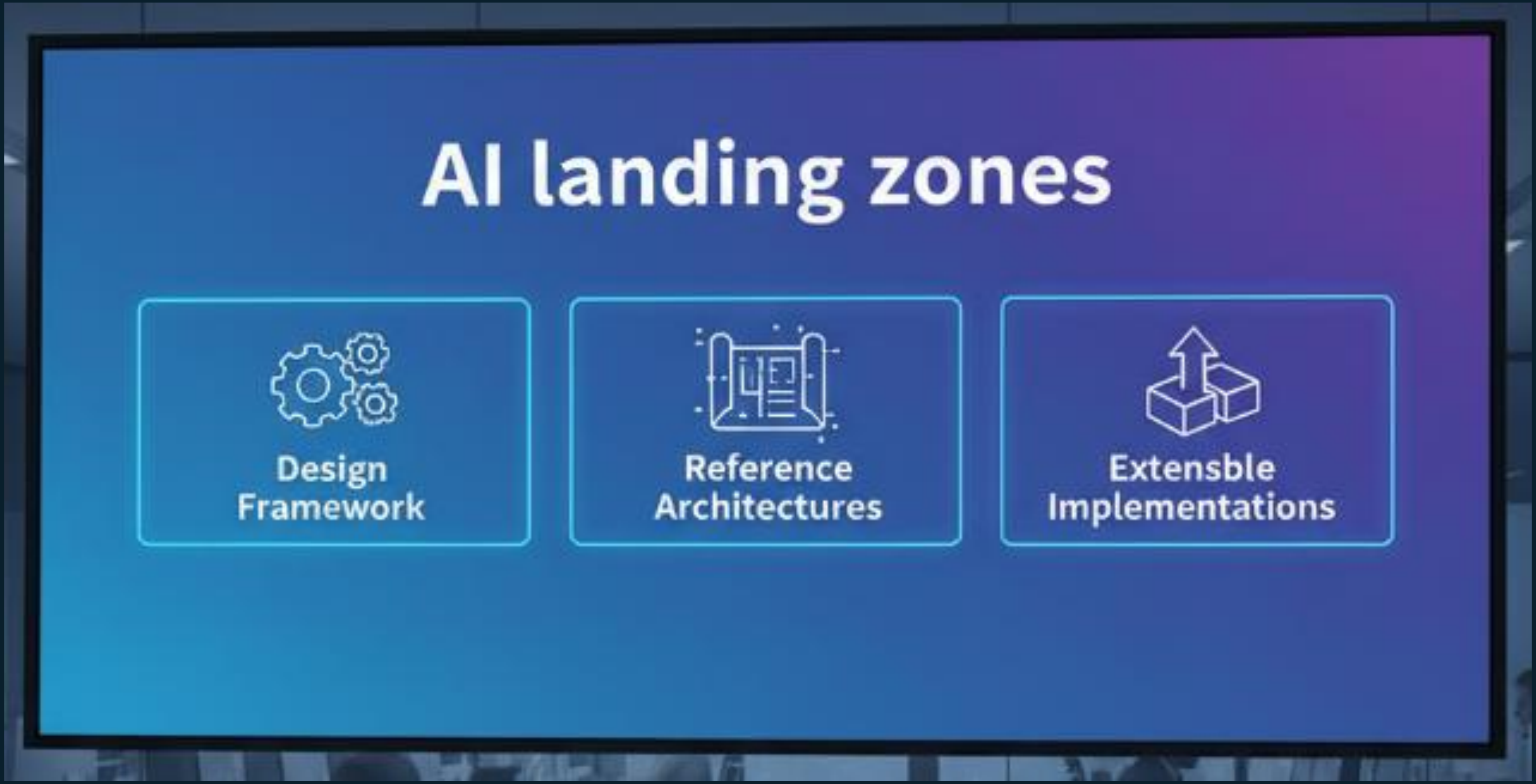
- Draft — Azure Monitor Ingestion limit alert — Medium · Medium · ALZ

+ Add item

AI Landing Zone Accelerator for AI Apps & Agents

Overview

An AI landing zone accelerator helps your team progress from proof-of-concept to scalable production environments faster by automating infrastructure setup using best practices from the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF).



AI landing zones

- Design Framework
- Reference Architectures
- Extensble Implementations

Design Checklist

Security

Identity

Compute

Data

Reliability

Networking

Governance

Monitoring

Cost Optimization

Platform Automation

Resource Organization

Operational Excellence

Performance Efficiency

Extensible Implementations

Terraform

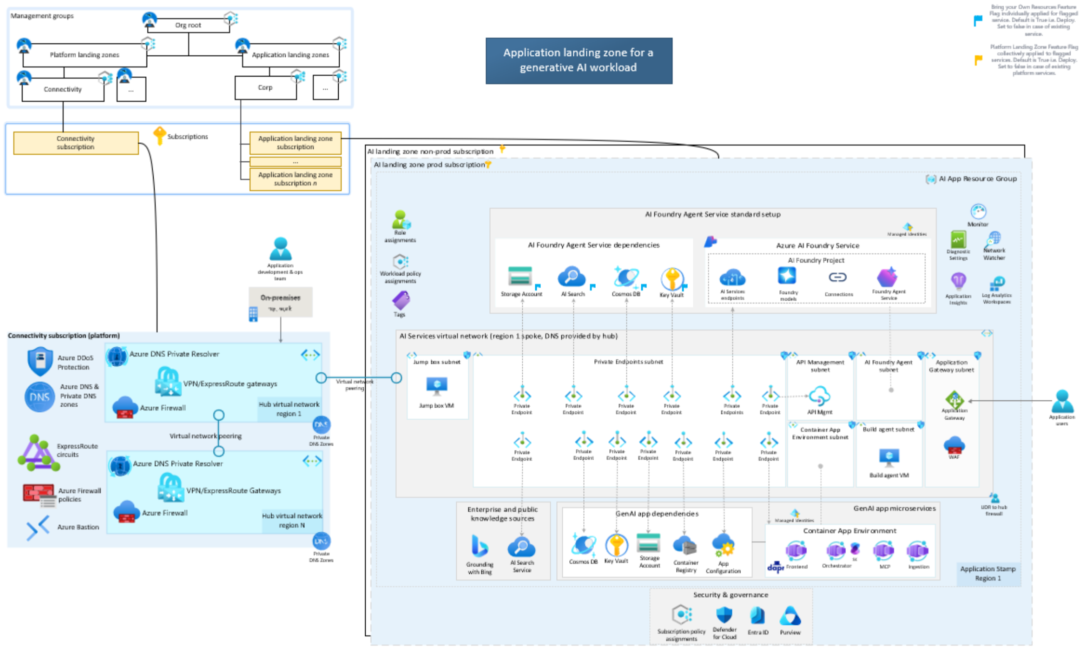
Bicep

Portal – Coming Soon

Reference Architectures

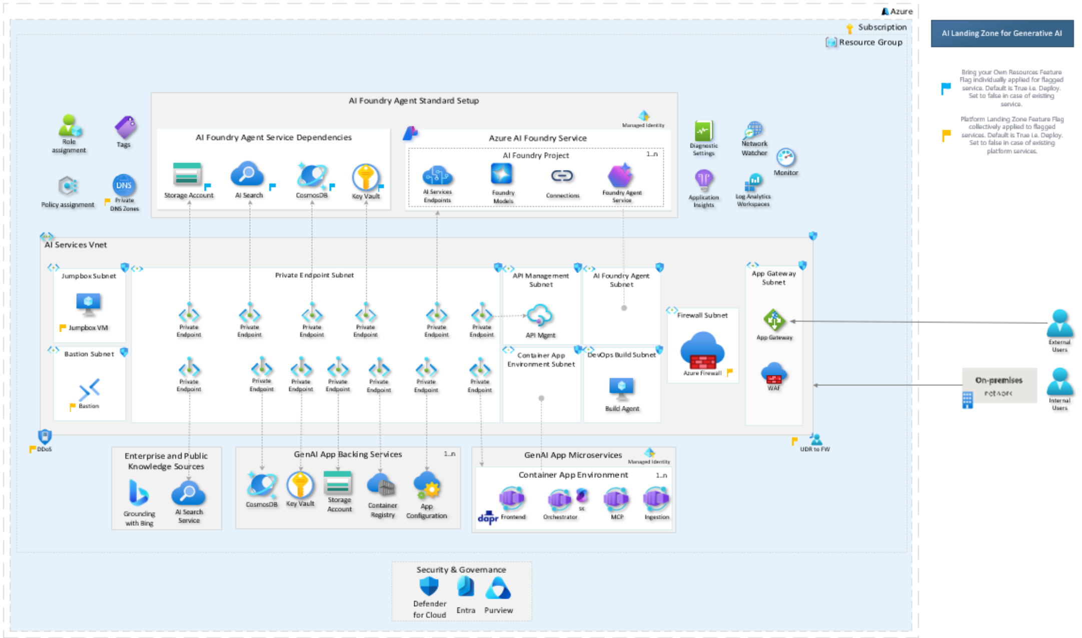
Enterprise-Scale and Production Ready to accelerate AI use cases

AI Landing Zone with Platform Landing Zone



Management groups
Org root
Platform landing zones
Application landing zones
Connectivity
...
Corp
...
Connectivity subscription
Subscriptions
Application landing zone subscription
...
Application landing zone subscription n
Application landing zone for a generative AI workload
Bring your Own Resources Feature Flag individually applied for flagged service. Default is True i.e. Deploy. Set to false in case of existing service.
Platform Landing Zone Feature Flag collectively applied to flagged services. Default is True i.e. Deploy. Set to false in case of existing platform services.
AI landing zone non-prod subscription
AI landing zone prod subscription
AI App Resource Group
Role assignments
Workload policy assignments
Tags
AI Foundry Agent Service standard setup
AI Foundry Agent Service dependencies
Storage Account
AI Search
Cosmos DB
Key Vault
Azure AI Foundry Service
AI Foundry Project
AI Services endpoints
Foundry models
Connections
Foundry Agent Service
Managed identities
Monitor
Diagnostic Settings
Network Watcher
Application Insights
Log Analytics Workspaces
Application development & ops team
On-premises
Connectivity subscription (platform)
Azure DDoS Protection
Azure DNS & Private DNS zones
ExpressRoute circuits
Azure Firewall policies
Azure Bastion
Azure DNS Private Resolver
VPN/ExpressRoute gateways
Azure Firewall
Hub virtual network region 1
Virtual network peering
Hub virtual network region N
Private DNS Zones
AI Services virtual network (region 1 spoke, DNS provided by hub)
Jump box subnet
Jump box VM
Private Endpoints subnet
Private Endpoint
API Management subnet
API Mgmt
AI Foundry Agent subnet
Application Gateway subnet
Application Gateway
WAF
Container App Environment subnet
Build agent subnet
Build agent VM
UDR to hub firewall
Application users
Enterprise and public knowledge sources
Grounding with Bing
AI Search Service
GenAI app dependencies
Cosmos DB
Key Vault
Storage Account
Container Registry
App Configuration
GenAI app microservices
Container App Environment
Frontend
Orchestrator
MCP
Ingestion
Application Stamp Region 1
Security & governance
Subscription policy assignments
Defender for Cloud
Entra ID
Purview

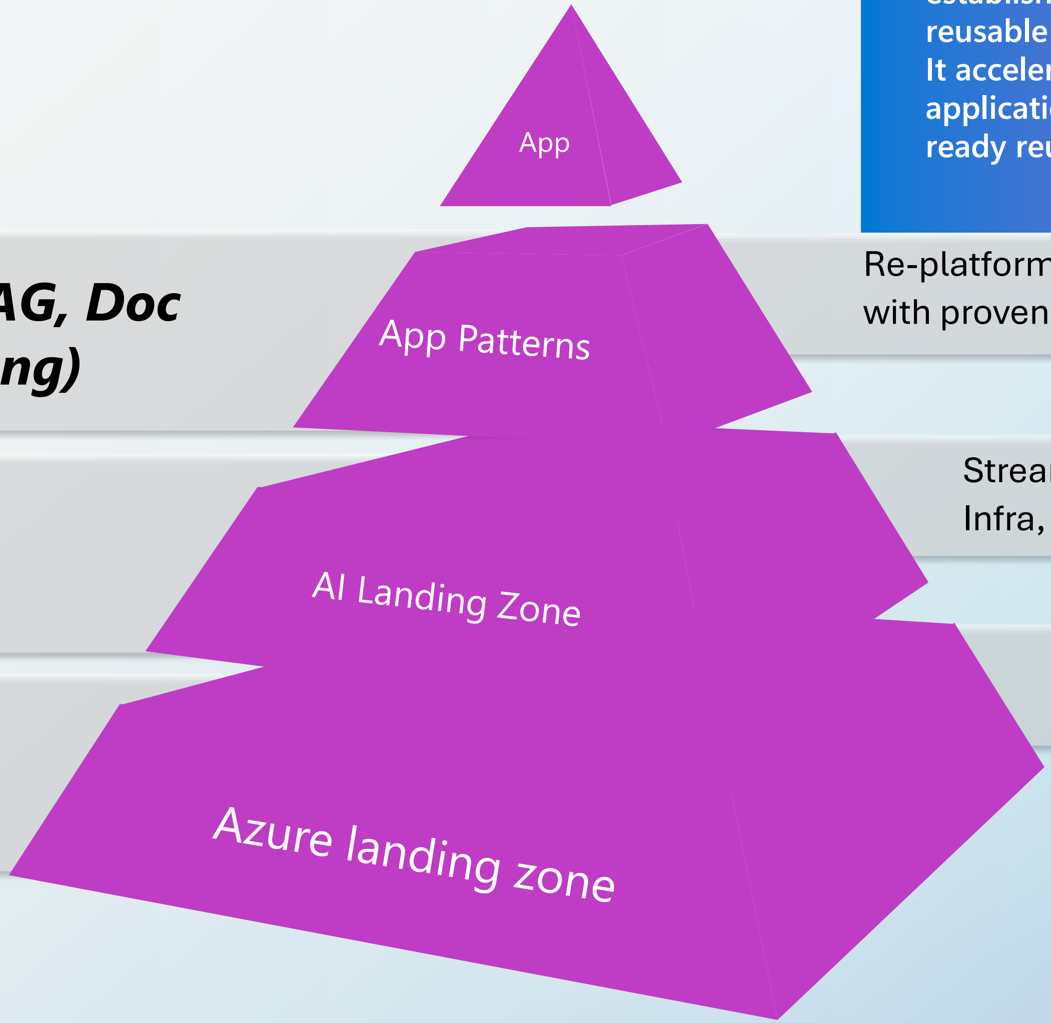
AI Landing Zone without Platform Landing Zone



Classified as Microsoft Confidential

AI Landing Zone Accelerator

AI Landing Zones offer prescriptive guidance, established cloud developer practices and offer reusable assets built upon Landing Zone Accelerators. It accelerates POC development and expedites application deployment by leveraging production ready reusable infrastructure files.



AI Use Cases (GPT-RAG, Doc Processing, Fine Tuning)

Re-platform .NET and Java apps with proven guidance.

Application Infrastructure

Streamline workload deployment for Infra, App, Data & Security

Platform Infrastructure

Set up secure, scalable well-governed cloud environment.

Authoritative resources for accelerating your app migration and modernization journey.

Explore AI Landing Zones

AI Landing Zone

aka.ms/AILZ

This month’s presenters:

Microsoft

Thank You! 👋

Stay up-to-date:

aka.ms/ALZ/WhatsNew

Microsoft

Q & A 😳

(yes, we are as shocked as you that we have time for this 😁)