NerdioCon 2025 PALM SPRINGS

Well-Architected AVD

Mastering Landing Zones with Nerdio

Agenda

Introduction

Understanding the Azure Virtual Desktop Well-Architected Framework

- Core pillars overview
- Key design areas of AVD

Implementing Azure landing zones for AVD deployments

Using Nerdio Manager in an AVD Well-Architected Framework with Landing Zones

Q&A session

Jeremy Wallace

Microsoft MVP | Azure
Principal Cloud Architect | Safari Micro
Certified Azure Solutions Architect Expert

mscloudbros.com

Youtube.com/@mscloudbros

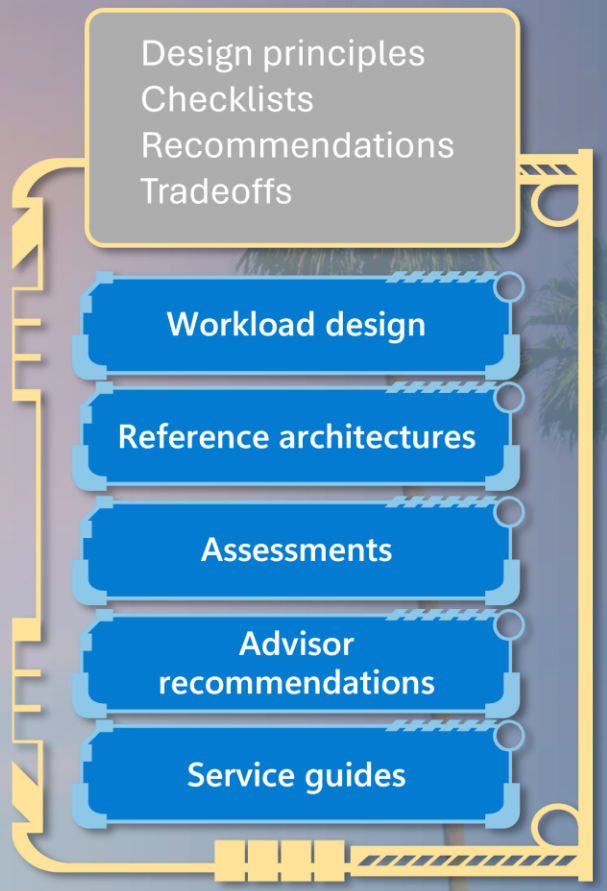
Andy Weidner

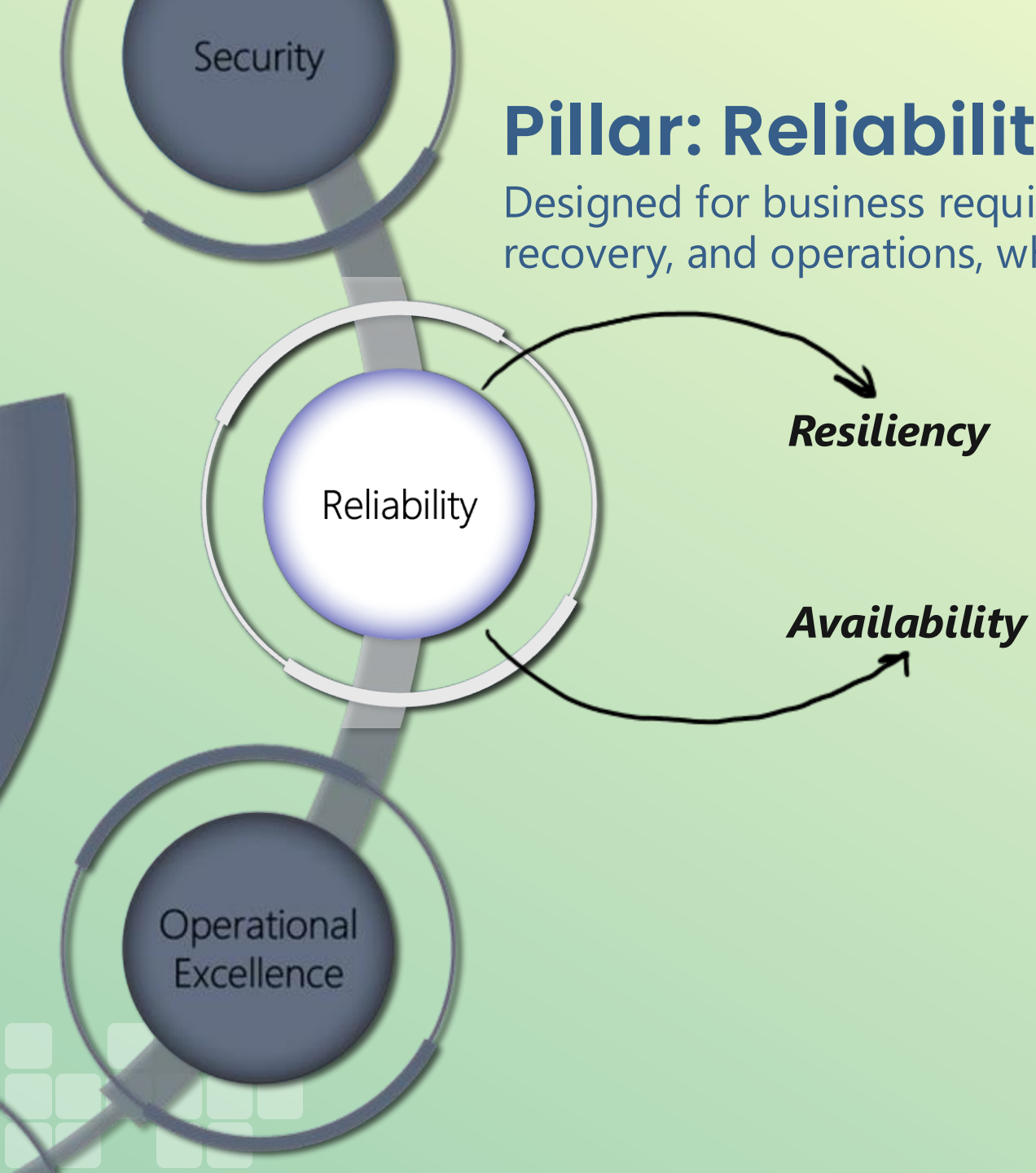
Product Manager | Nerdio

nerdio

ISC2 CISSP®

Well-Architected Framework





Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Resiliency

Availability

Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Feature	Resiliency	Availability
Focus	Recovery after failure	Ensuring uninterrupted uptime
Goal	Minimize data loss and restore operations	Keep AVD accessible even during issues
Example Failure Scenarios	VM crash, storage corruption, profile loss	Planned maintenance, session host overload, data center outage
Solutions in AVD	FSLogix backups, redundant storage, autoscaling	Multi-zone deployment, autoscaling, load balancing
Metric	Recovery Time Objective (RTO) – Time to restore service	Uptime Percentage (99.9% SLA)

Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Define service-level agreements (SLAs)
Establishing well-defined SLAs is central to fostering reliability. These agreements specify precise expectations for the availability and performance of user sessions and profiles.

Users should have uninterrupted access to virtual desktops for at least X% of business hours.

Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Define service-level agreements (SLAs)

Performance

Latency

"Session launch should be under x seconds"

Response Times for applications

"under x ms for critical apps"

Profile Load times

"FSLogix Profile loading within x seconds."

Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Define service-level agreements (SLAs)

Scalability

“Maximum time allowed for provisioning new session hosts in response to increased demand is x minutes.”

Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Define service-level agreements (SLAs)

Disaster recovery & business continuity

Recovery Time Objective (RTO)

“If a session host fails, a new one should be available within x minutes.”

Recovery Point Objective (RPO)

“User data should never be lost beyond the last x minutes due to backups and replication.”

Pillar: Reliability

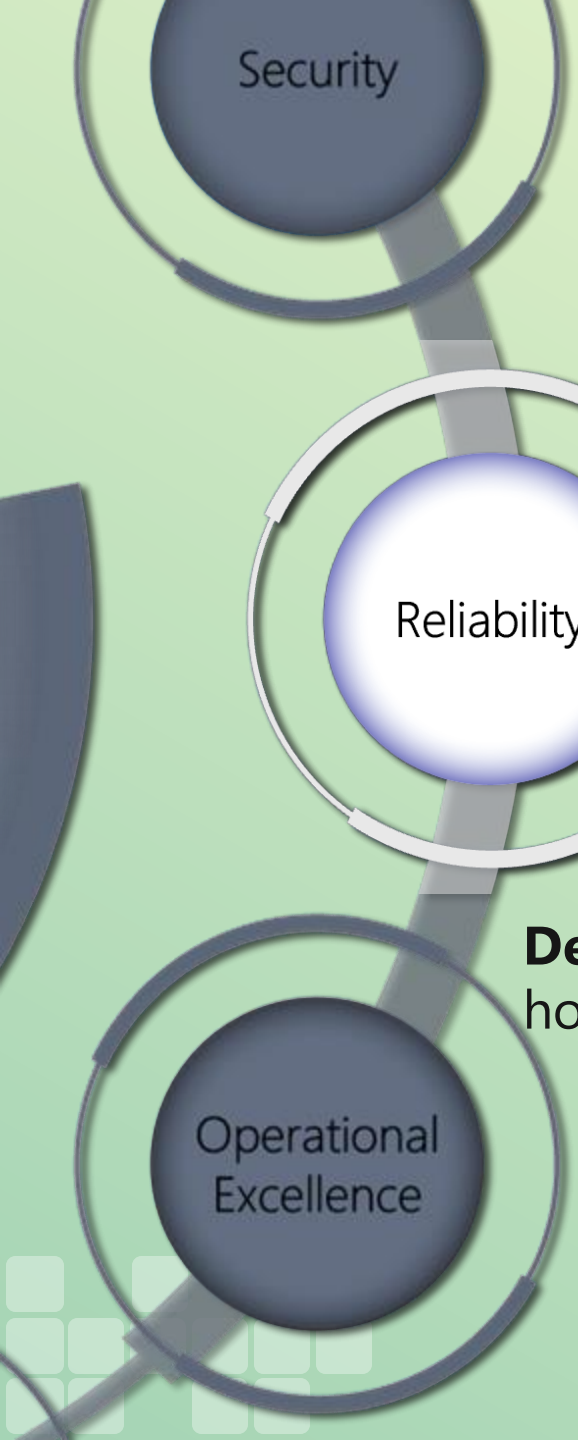
Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Define service-level agreements (SLAs)

Support and incident response

Critical (e.g., AVD outage): Response within x minutes.
High (e.g., major performance degradation): Response within an hour.
Medium (e.g., individual user session issue): Response within x hours.

Define escalation procedures and responsibilities for IT teams.



Pillar: Reliability

Designed for business requirements, resilience, recovery, and operations, while keeping it simple.

Define service-level agreements (SLAs)

Develop effective scaling strategies
horizontal scaling, vertical scaling

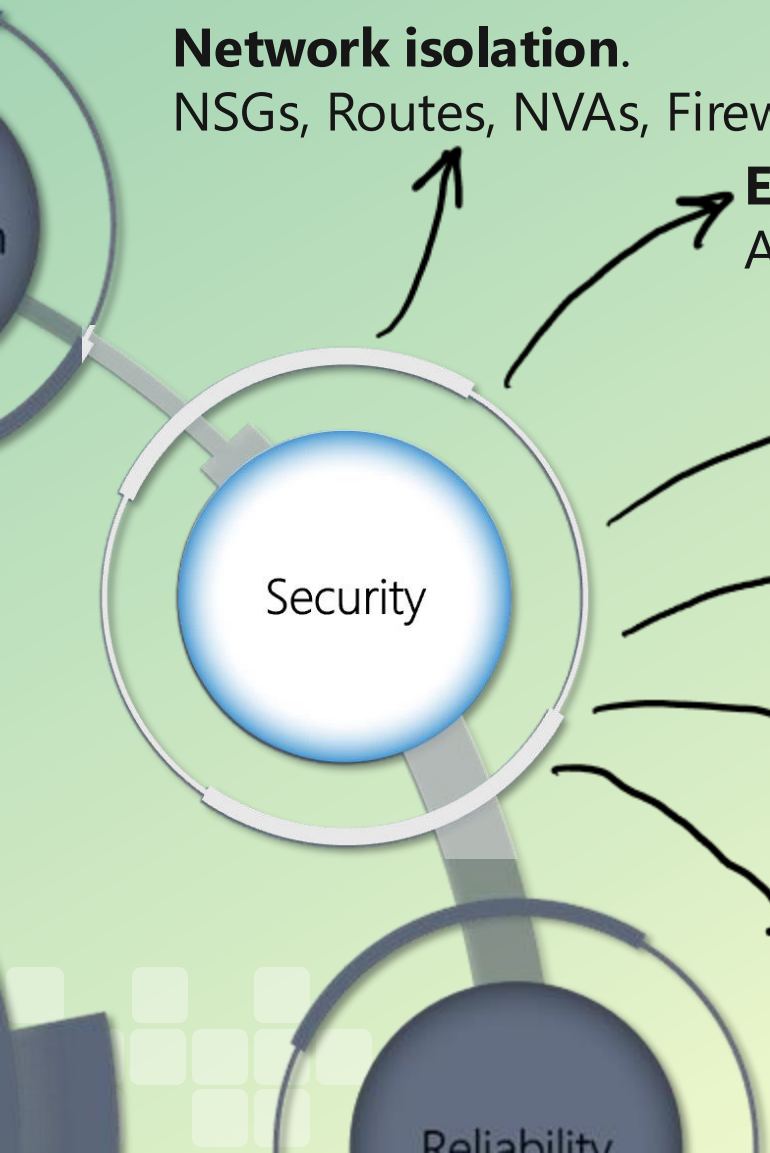
Design for high availability
base hosts

Implement fault tolerance.
FSLogix on Azure Files with ZRS/GRS

Understand backup and restore capabilities
ASR, Azure Backup

Pillar: Security

Protect confidentiality, integrity, and availability.



Network isolation.
NSGs, Routes, NVAs, Firewalls

Environmental audits.
Are you verifying security is in place?

Patch management.
Windows Updates, app updates

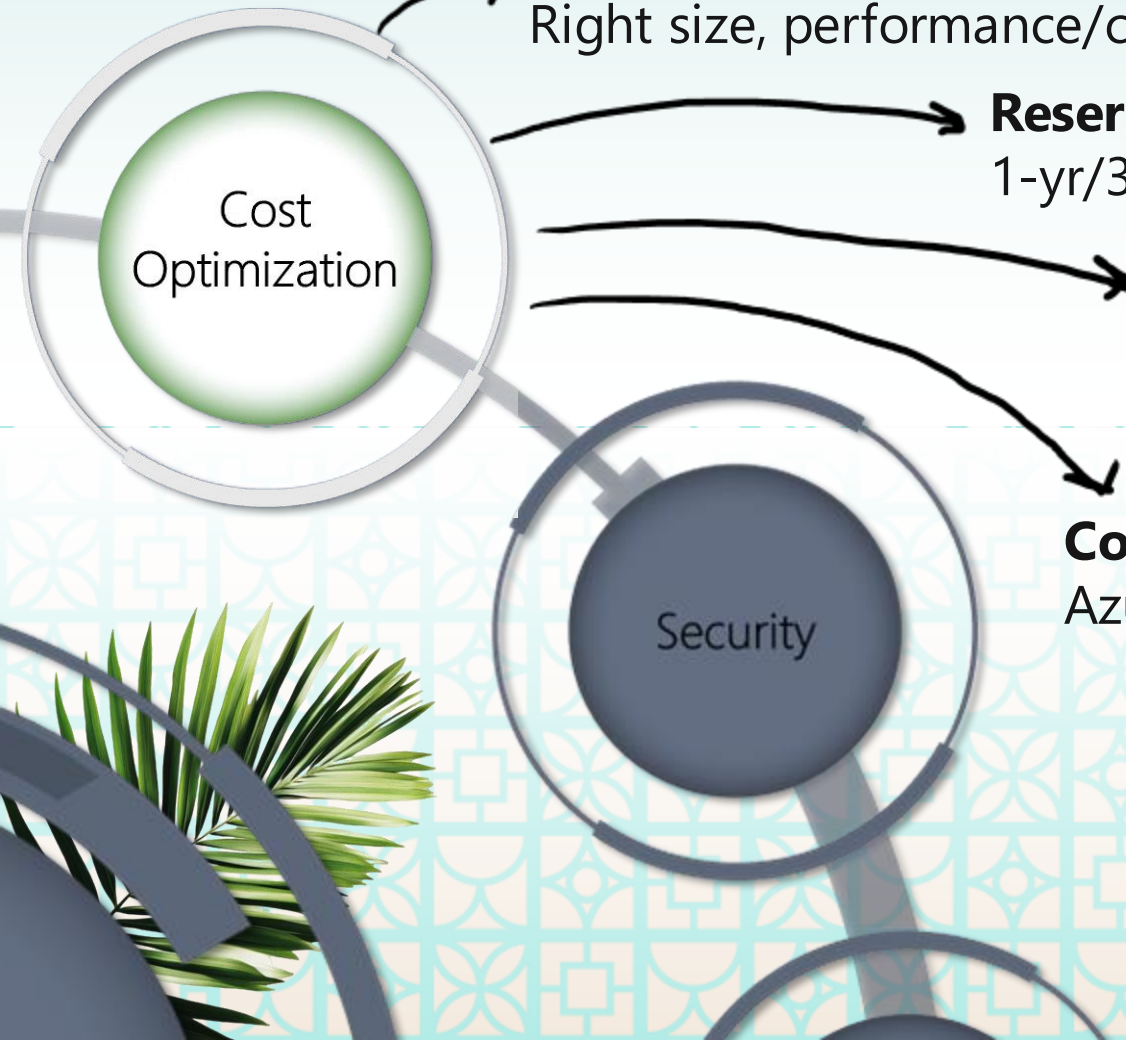
Security information and event management (SIEM)
Microsoft Sentinel

Data encryption
Azure Disk Encryption, Confidential computing

Identity and access management.
MFA, Entra DS, Entra ID, ADDS

Pillar: Cost Optimization

Optimize on usage and rate utilization while keeping a cost-efficient mindset.



Using cost-effective VMs
Right size, performance/cost

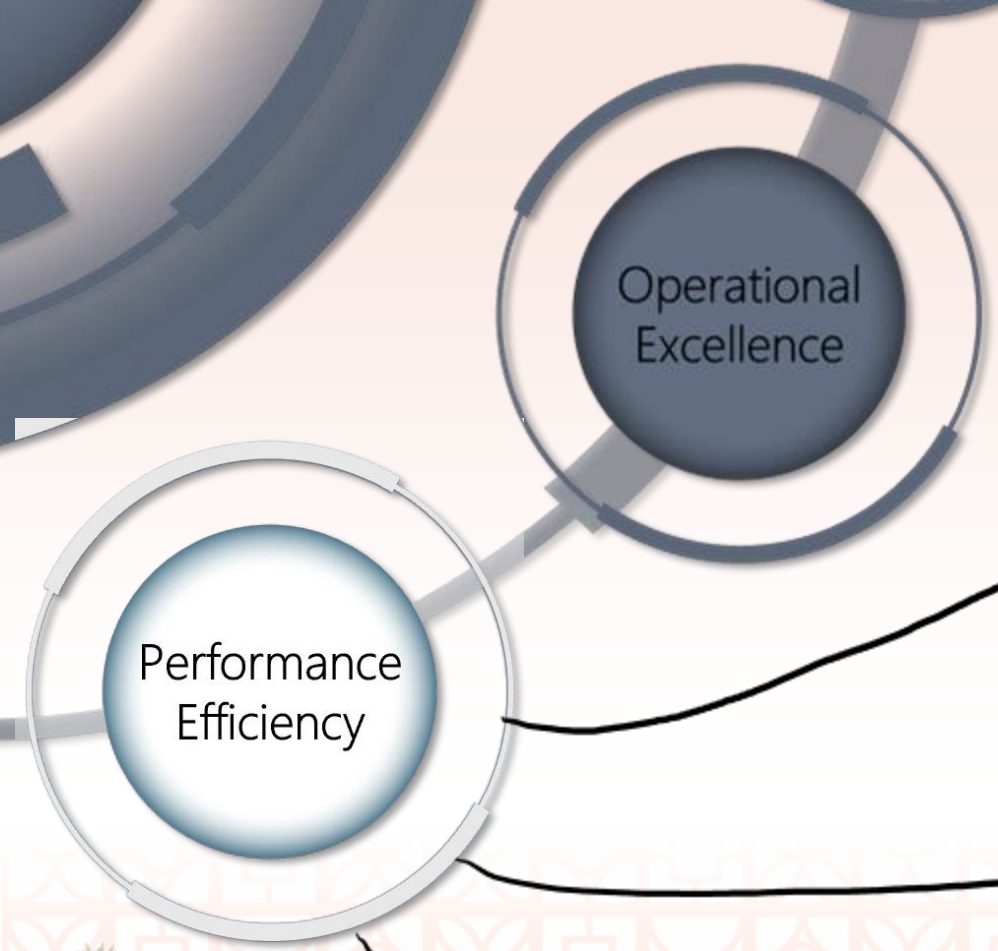
Reserved instances or savings plans
1-yr/3-yr RI, Azure Advisor

Fine tuned Autoscaling
Pre-stage & scale in times, triggers, base, & active

Cost analysis/tracking/management
Azure Cost Management

Pillar: Performance efficiency

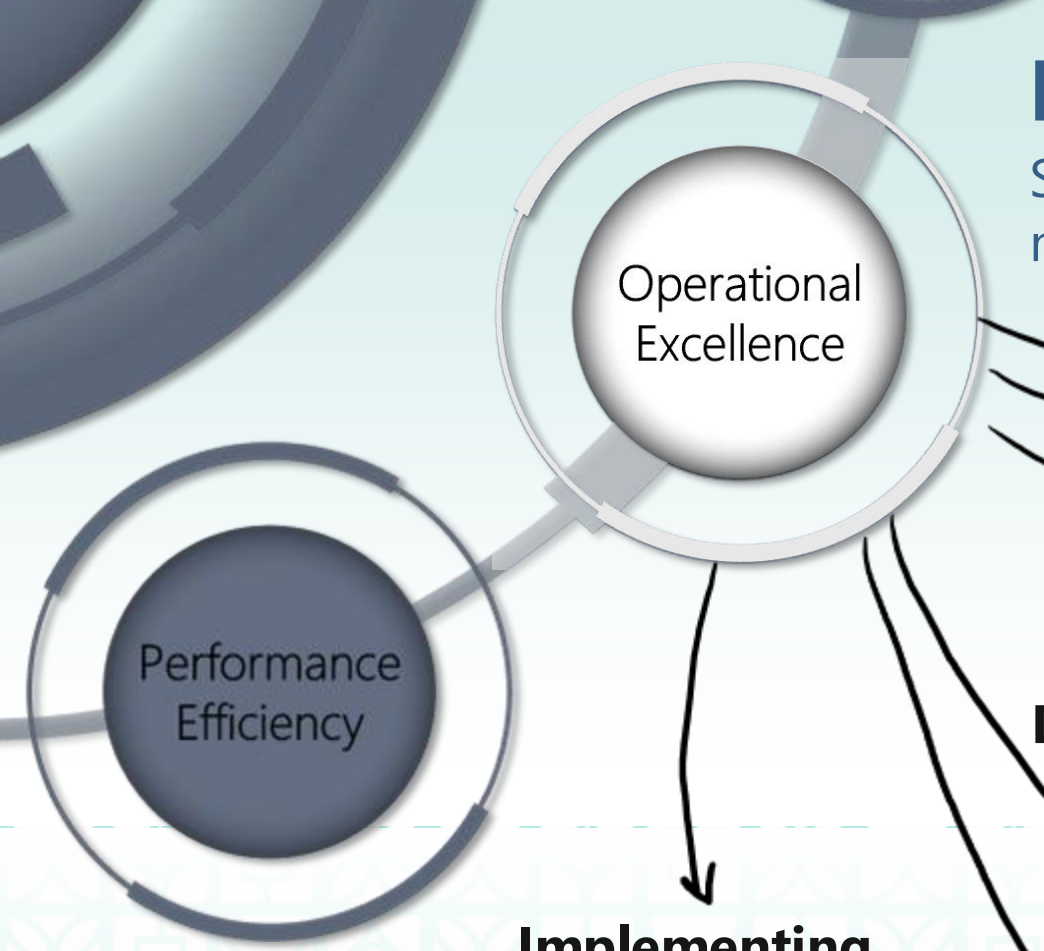
Optimizing workloads—Scale horizontally, test early and often, and monitor the health of the solution.



Allocating the proper size, family, and number of session hosts

Continuously monitoring performance and detecting anomalies by using tools such as Azure Monitor, Log Analytics, Application Insights, and alerts

Configuring a proper scaling so that you have an ideal number of session hosts available for users



Pillar: Operational excellence

Streamline operations with standards, comprehensive monitoring, and safe deployment practices.

Using IaC for repeatable, consistent deployment

Proper monitoring of resources to maintain the health of your environment

Documentation

An adequate continuous integration/continuous delivery (CI/CD) pipeline

Implementing Azure policy-driven governance to help ensure security and compliance

Designing an RBAC delegation schema

Maintaining governance and compliance standards for your host pool

Key design Aareas for Well-Architected AVD

Application delivery

Application delivery

Host pool types *(Cost optimization, reliability)*
- **Personal pools**: Persistent user environment
- **Pooled pools**: Cost-efficient, shared resources

Load-balancing algorithms *(Cost optimization, performance efficiency)*
- **Breadth-first**: Enhances user experience
- **Depth-first**: Maximizes resource utilization

Scaling plans *(Cost optimization, performance efficiency)*
- Automatically adjust host availability
- Optimize scaling settings for cost efficiency

Regions *(Reliability, performance efficiency)*
- Deploy session hosts near users
- Use availability zones for resiliency

Compute size *(Cost optimization, performance efficiency)*
- Match VM size to workload needs
- Use specialized VMs (GPU, secure types)

Storage solutions *(Cost optimization, performance efficiency)*
- Select optimal disk type and size
- Balance performance and cost efficiency

Fault tolerance *(Cost optimization, reliability)*
- Distribute hosts across availability zones
- Implement DR (golden images or backups)

Key design areas for Well-Architected AVD

Networking & connectivity

Networking & connectivity

Client latency *(Performance efficiency)*
- Measure latency with Azure testing tools (Latte, SockPerf)
- Use RDP Shortpath and UDP-based split tunneling

On-premises connectivity *(Performance efficiency, operational excellence)*
- Assess bandwidth and latency needs for hybrid connections
- Avoid IP conflicts; design subnets for growth

Multi-region connectivity *(Performance efficiency, cost optimization)*
- Replicate critical services across regions
- Choose VMs with accelerated networking to reduce latency

Network security *(Security, operational excellence)*
- Adopt identity-driven security over traditional perimeters
- Implement security groups, Azure Firewall, and service tags

Private endpoints (Private Link) *(Security)*
- Use Azure Private Link for internal connectivity
- Configure DNS for private endpoints

RDP Shortpath *(Performance efficiency, cost optimization)*
- Enable direct UDP connections for lower latency
- Understand managed/unmanaged network connection options

Key design areas for Well-Architected AVD

Monitoring

Monitoring

Health & availability
(Reliability, operational excellence)
- Use Service Health for Azure outage alerts
- Monitor VMs and storage with Resource Health

Performance monitoring
(Performance efficiency, operational excellence)
- Configure diagnostics in Log Analytics
- Track key VM metrics and storage thresholds

Security monitoring *(Security)*
- Enable Defender for Cloud and Sentinel
- Regularly review logs, security updates, and compliance

Reporting *(Operational excellence)*
- Use Azure Virtual Desktop Insights dashboards
- Create custom reports with Log Analytics data

Alerting
(Performance efficiency, operational excellence)
- Set proactive alerts for performance issues
- Monitor critical Azure Virtual Desktop events

Key design areas for Well-Architected AVD

Security & IAM

Security & IAM

Role-Based Access Control (RBAC) *(Security, operational excellence)*

- Define roles clearly (built-in/custom)
- Use security groups for role assignment

Session host security *(Security)*

- Restrict user access and software (AppLocker, screen capture protection)
- Enable Microsoft Defender, Application Control, and auto-sign-out

Identity and networking *(Security)*

- Enforce MFA and Conditional Access
- Implement hub-spoke architecture and isolate networks

Data encryption in transit *(Security)*

- Ensure TLS 1.2 compatibility between clients and hosts
- Understand Azure Virtual Desktop encryption methods

Confidential computing *(Security, performance efficiency)*

- Use confidential VMs (DCasv5, ECasv5) for regulated industries
- Protect sensitive data during active processing

Key design areas for Well-Architected AVD

Operational procedures

Operational procedures

Shared responsibilities
(Operational excellence, performance, security)
- Understand Microsoft vs. customer-managed components
- Actively manage your network, session hosts, and workspaces

Environment management
(Operational excellence, reliability)
- Deploy session hosts with availability zones
- Establish operational baselines and proactive monitoring

Awareness of updates *(Operational excellence)*
- Regularly review Azure Virtual Desktop updates
- Monitor monthly release notes

Monitor limit thresholds *(Operational excellence)*
- Track resource limits (VMs, vCPUs, FSLogix IOPS)
- Automate VM token refresh to prevent expirations

Golden Image updates
(Operational excellence, reliability)
- Deploy second host pool for low-risk updates
- Manage updates carefully to avoid capacity issues

Image management
(Operational excellence, security)
- Automate golden image updates with VM Image Builder
- Use Azure Marketplace, scripts, and Key Vault for security

Version compliance *(Operational excellence)*
- Regularly review component release notes
- Promptly install available updates

Key design areas for Well-Architected AVD

Business continuity

Business continuity

Azure Virtual Desktop Service *(Reliability)*

- Know shared responsibilities (Microsoft vs. customer-managed)
- Proactively manage your VMs, profiles, and settings

Host pools *(Reliability, cost optimization)*

- Use active-active or active-passive host pool configurations
- Sync profiles across regions with FSLogix Cloud Cache

Capacity planning *(Reliability, cost optimization)*

- Monitor Azure subscription and VM limits
- Plan horizontal scaling and use multiple subscriptions if needed

FSLogix profiles and App Attach *(Reliability, cost optimization)*

- Minimize profile data; back up profiles with Azure Backup
- Use zone-redundant storage and FSLogix Cloud Cache

Virtual networks *(Reliability, cost Ooptimization)*

- Configure a virtual network in secondary region for failover
- Utilize Azure Site Recovery for network replication

Golden Images *(Reliability, cost optimization)*

- Store and replicate images with Azure Compute Gallery
- Use zone-redundant storage; maintain secondary gallery in alternate region

Key design areas for Well-Architected AVD

Storage

Storage

Region relection
(Performance efficiency, cost optimization)

- Verify VM SKU availability and compliance requirements
- Deploy storage resources in the same region as host pools to reduce latency

Applications (App Attach) *(Operational excellence)*

- Use App Attach for flexible, efficient application deployment
- Separate App Attach storage from FSLogix; plan permissions and disaster recovery carefully

VM and disk sizing
(Performance efficiency, cost optimization)

- Right-size VMs (CPU, GPU, memory, storage) based on workloads
- Use scaling plans; choose SSD disks for optimal performance and SLAs

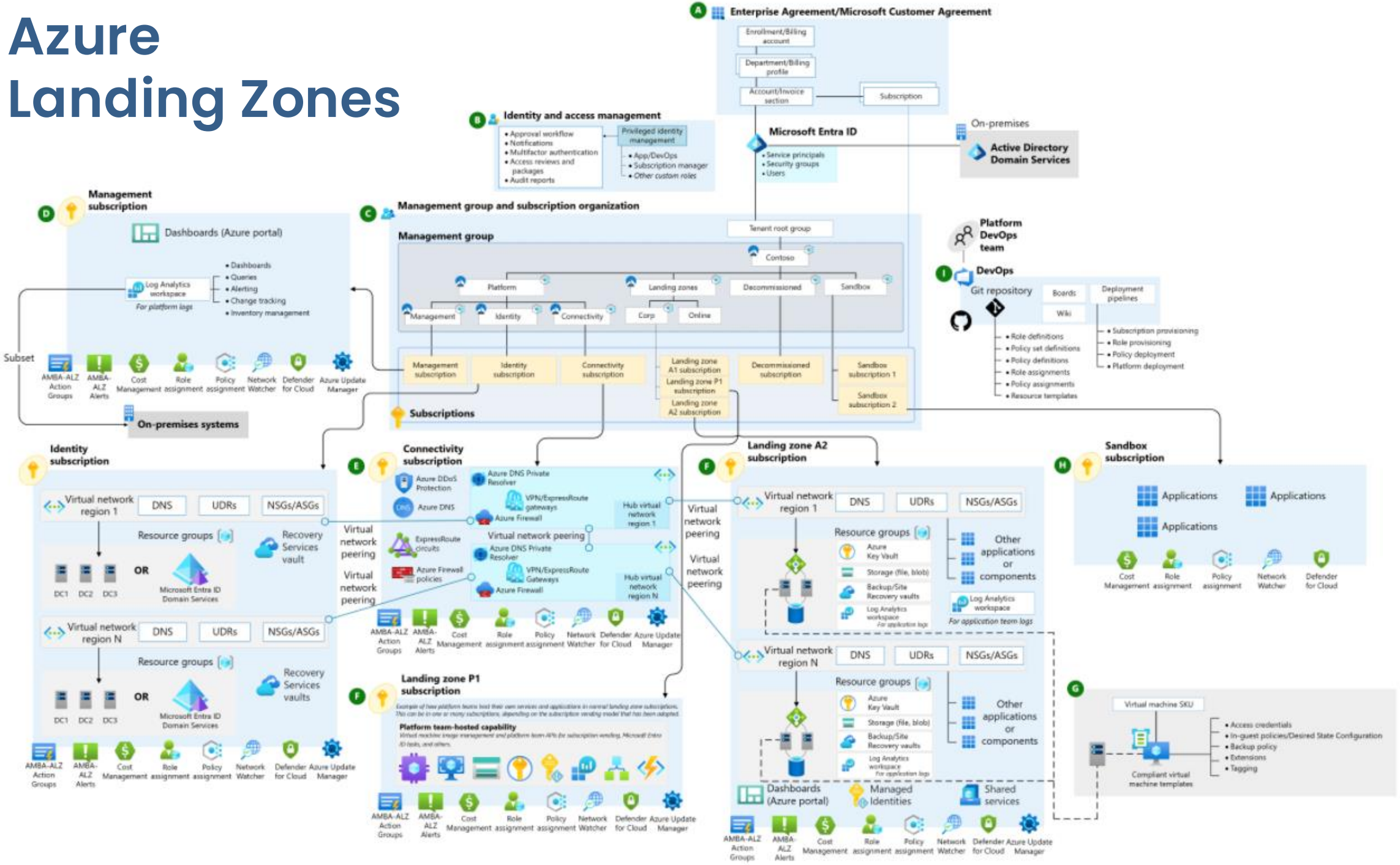
User profiles (FSLogix)
(Performance efficiency, cost optimization)

- Use FSLogix for efficient profile management
- Prefer Azure Files; consider Azure NetApp Files for large-scale or high-performance scenarios

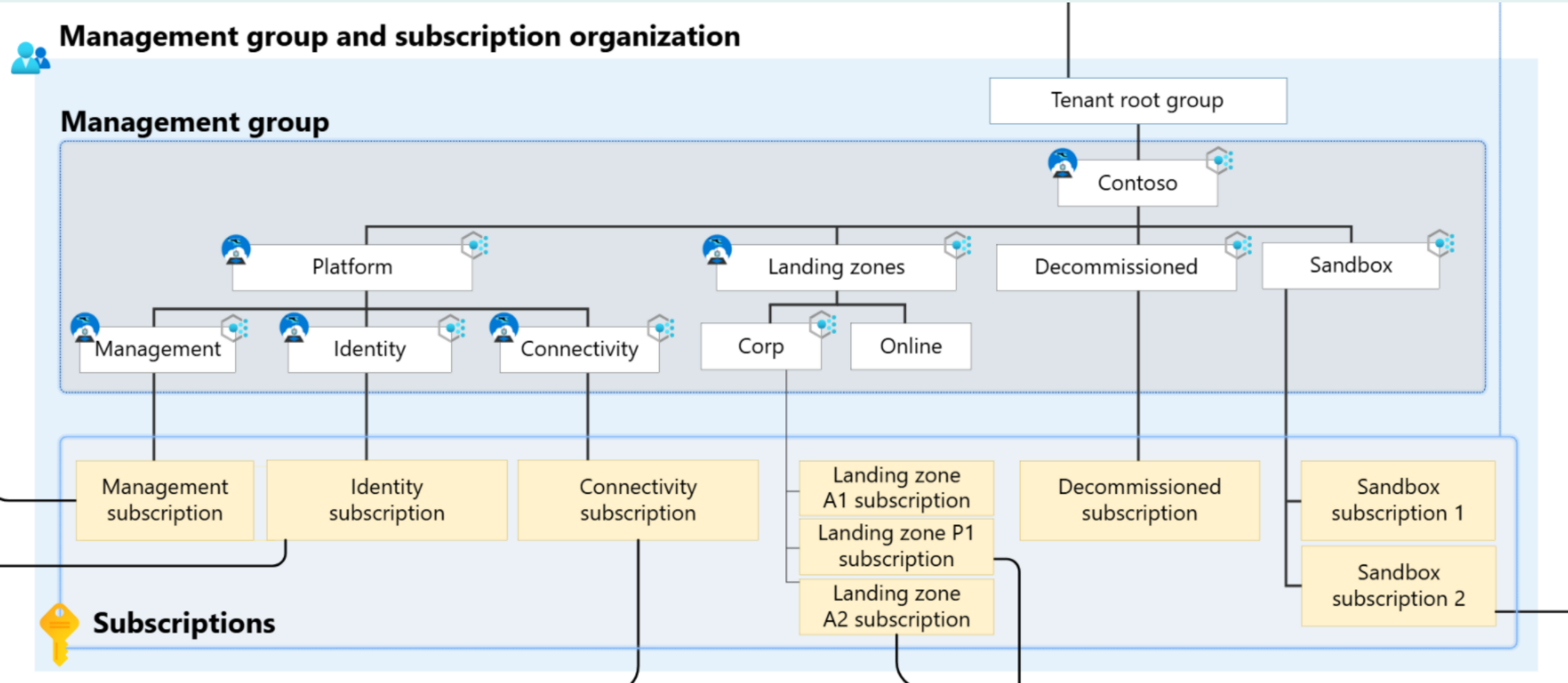
NerdioCon 2025 PALM SPRINGS

Azure Landing Zones

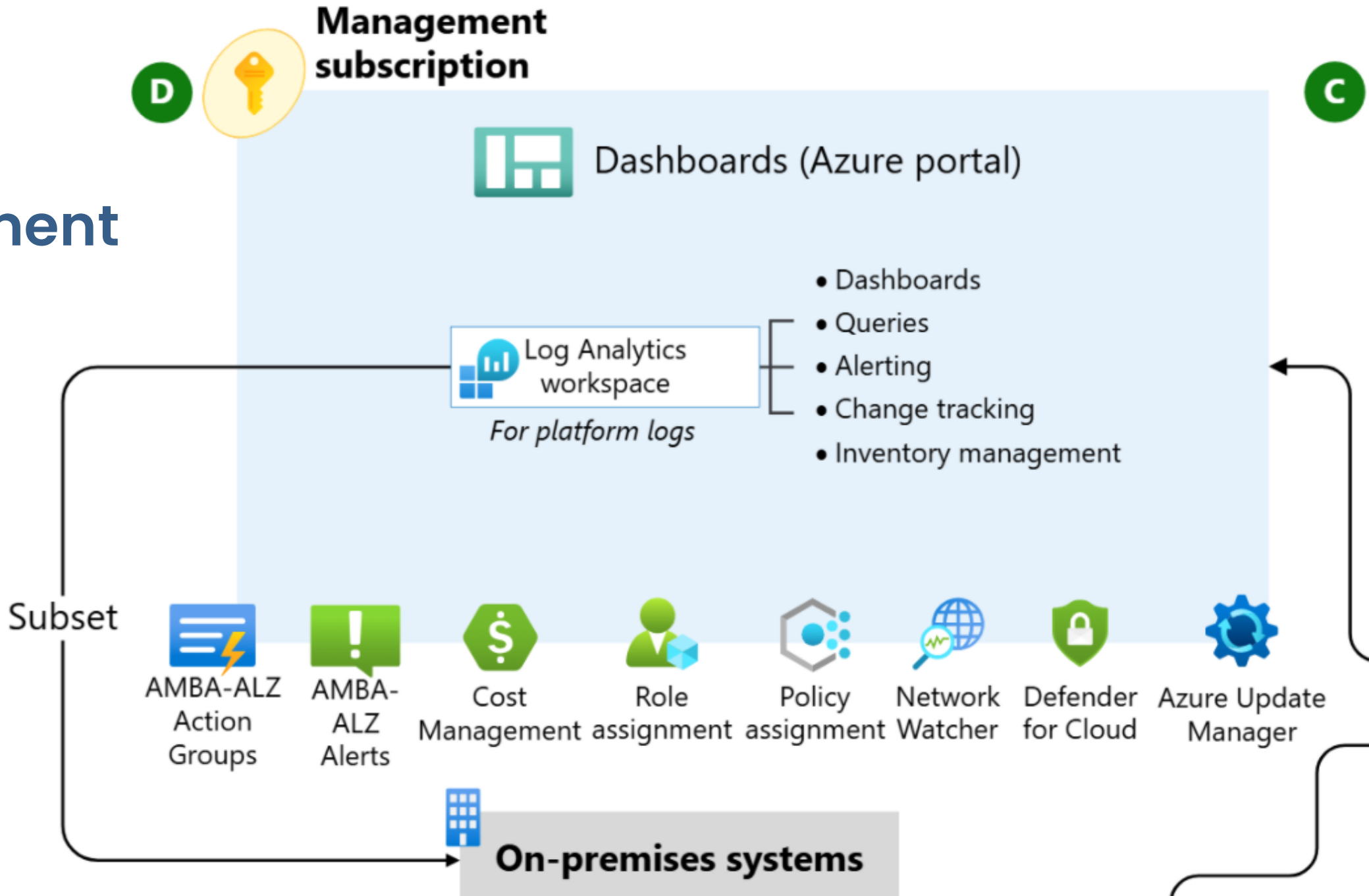
Azure Landing Zones



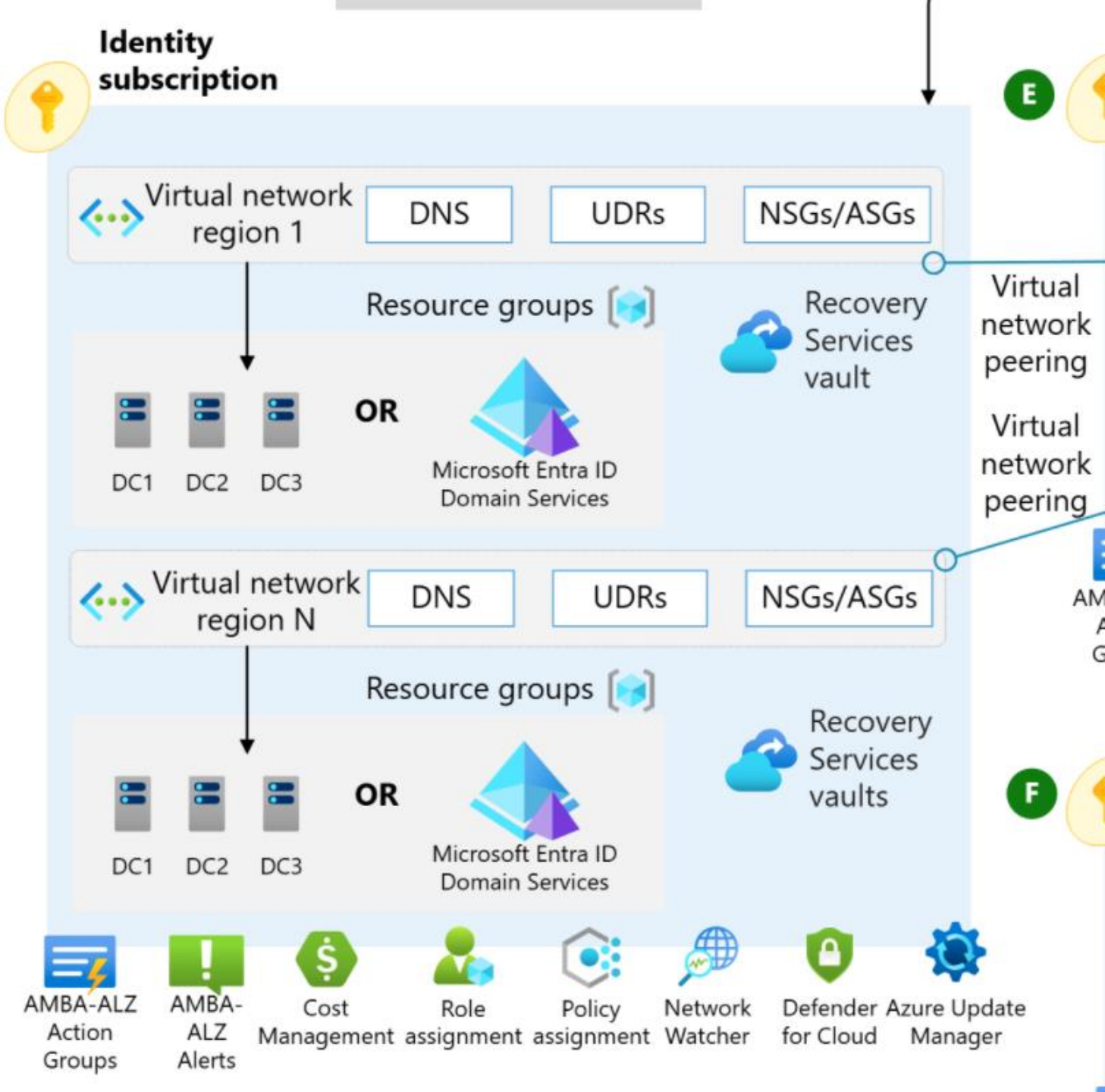
Management groups & Azure subs



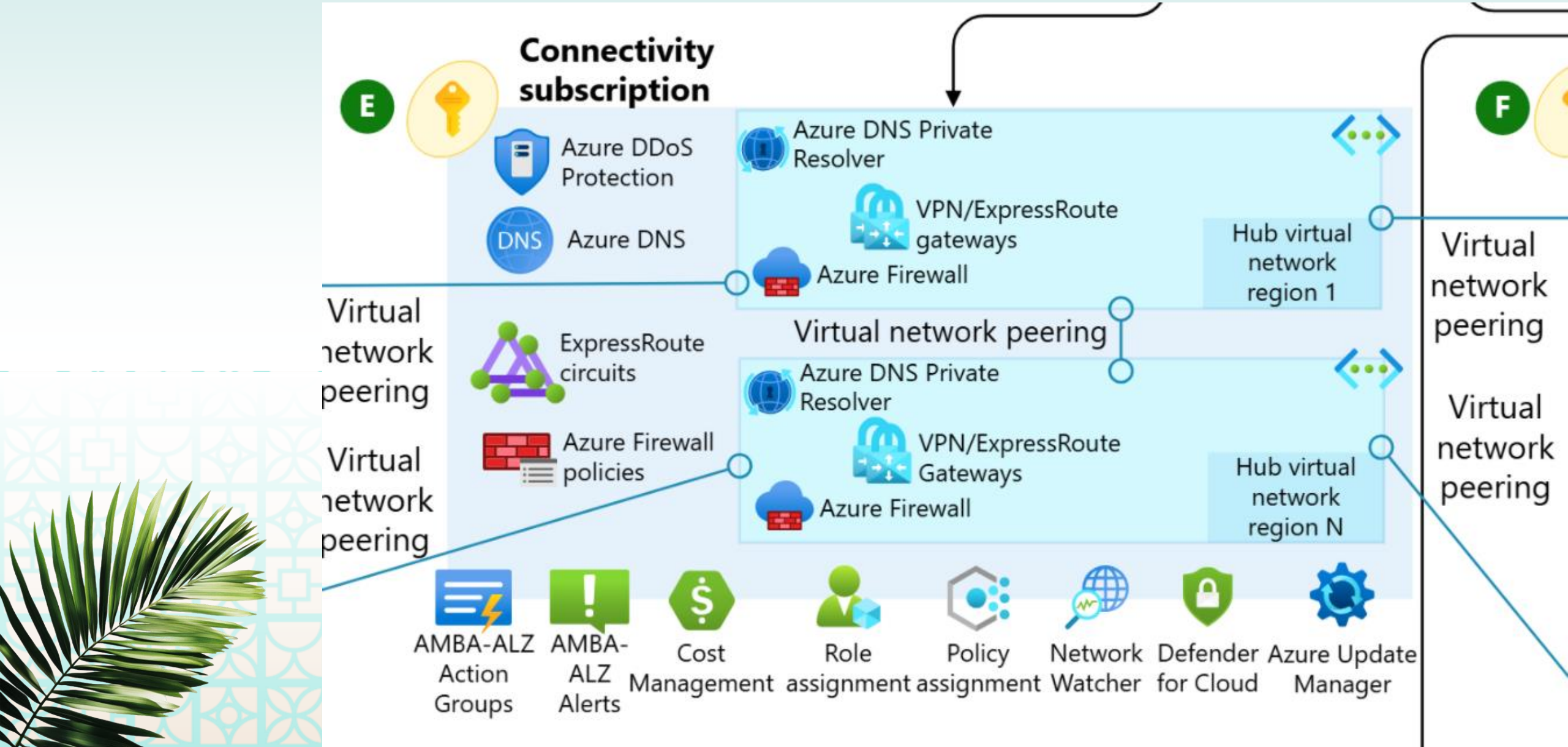
Management platform



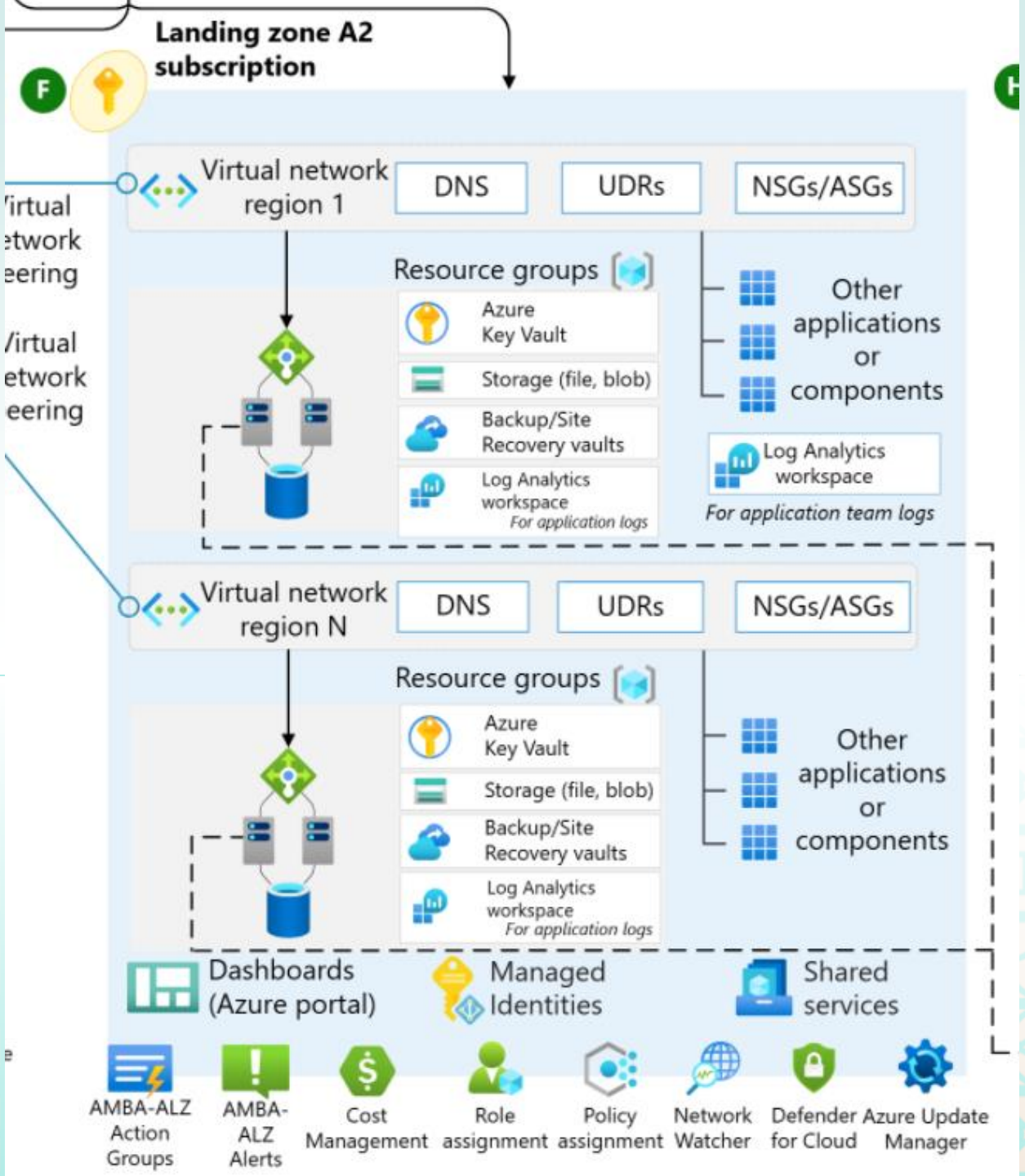
Identity platform



Connectivity platform

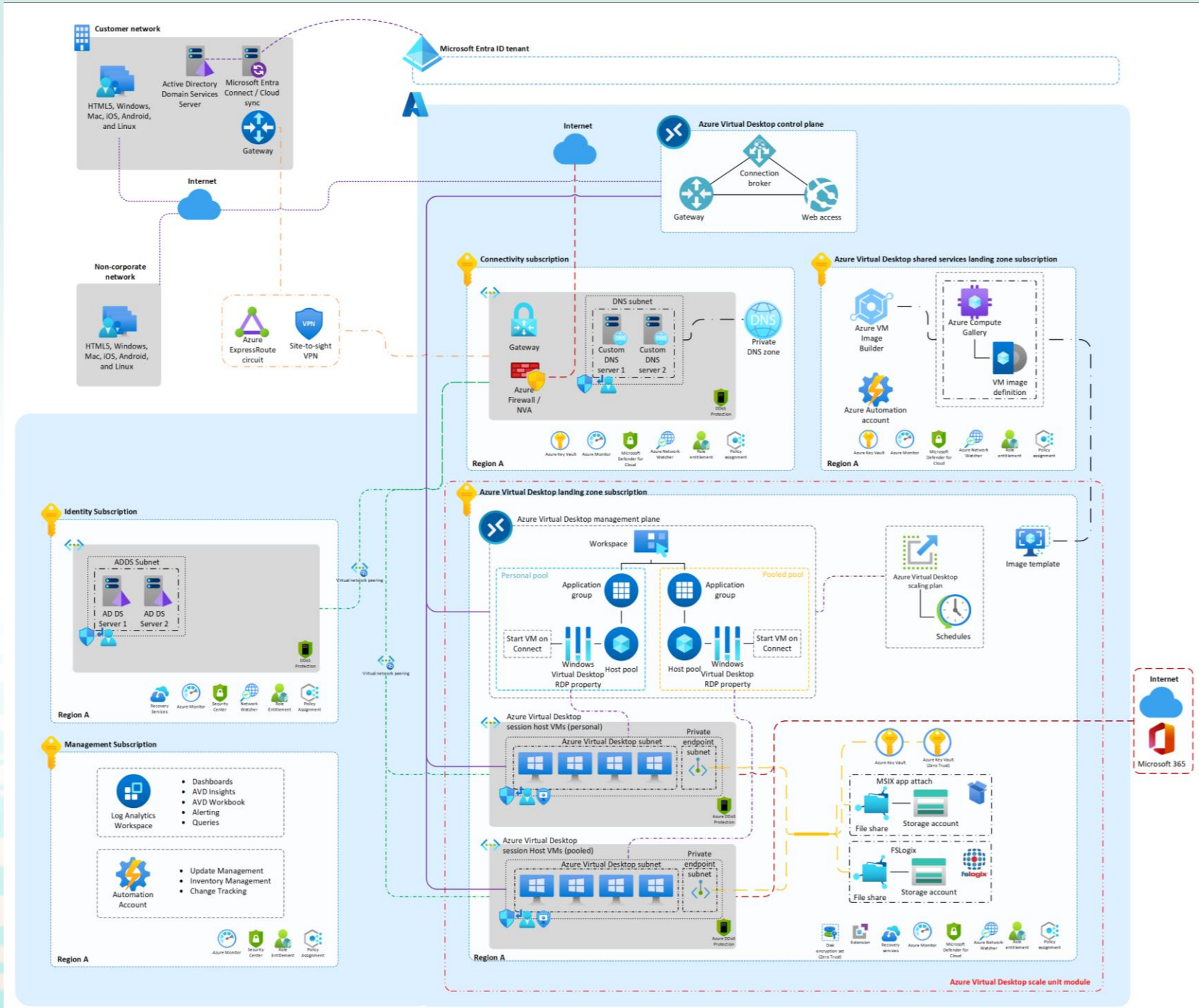


Application Landing Zone

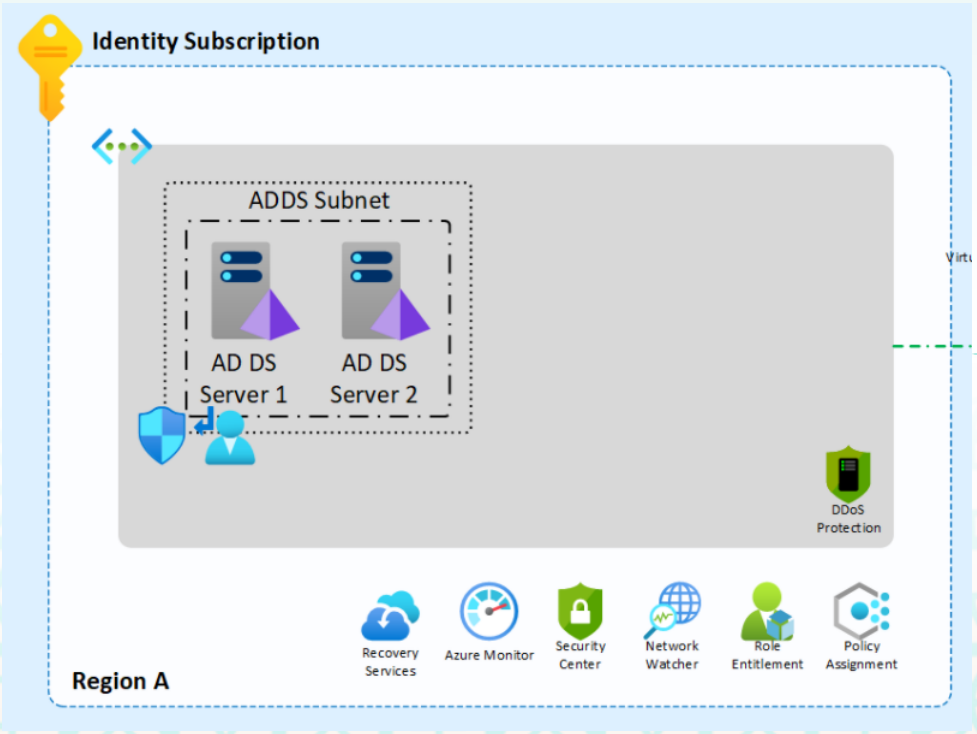


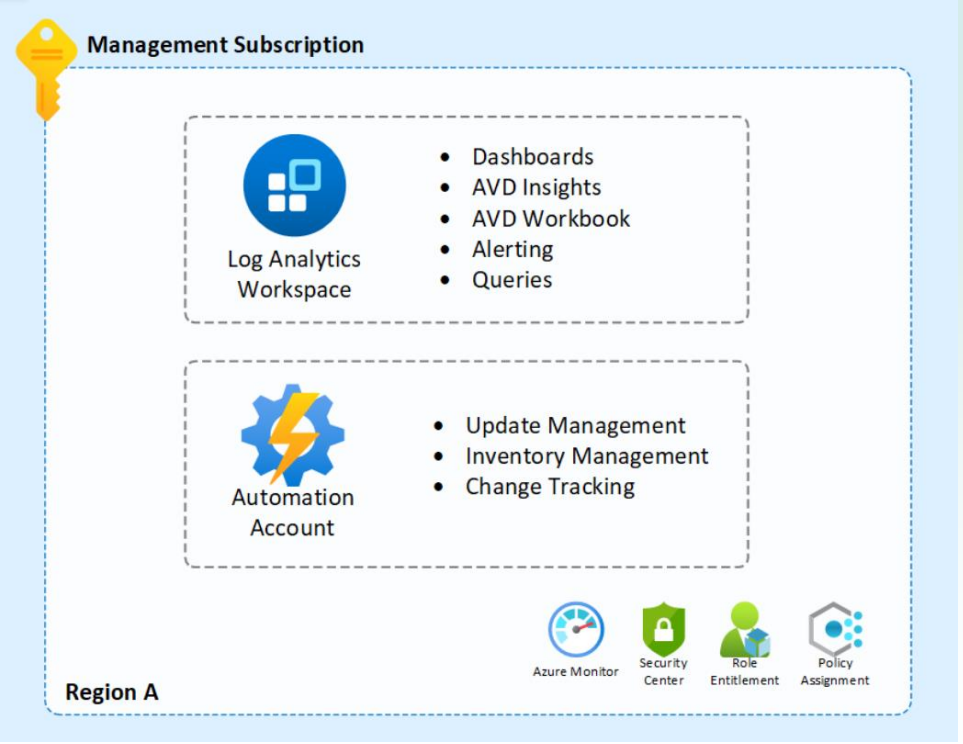
Azure Landing Zones

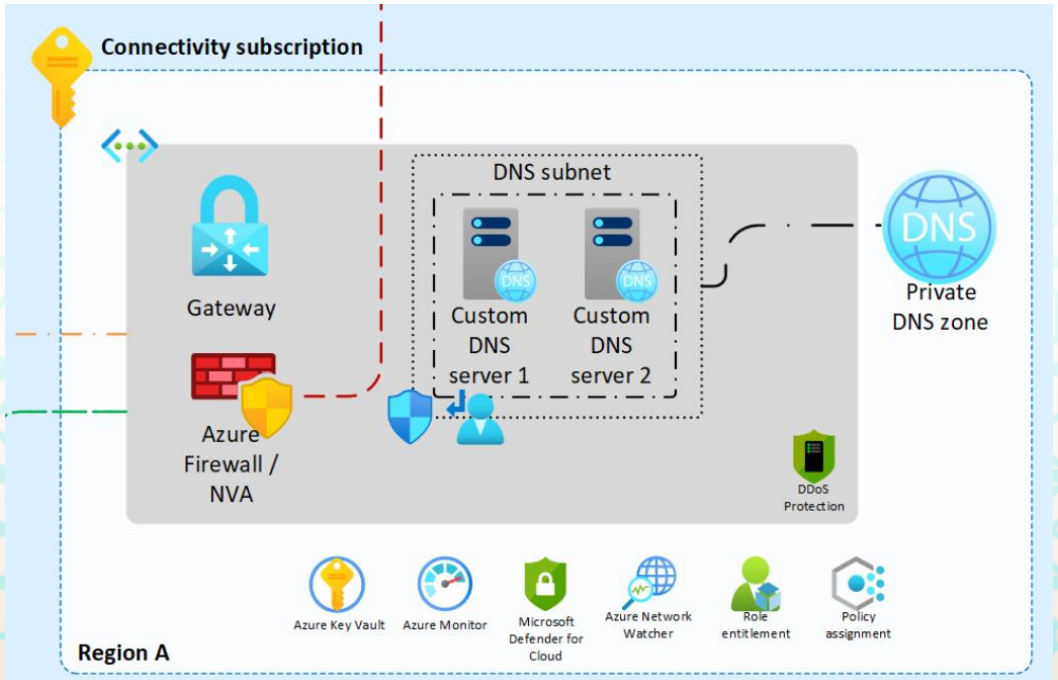
AVD Focus



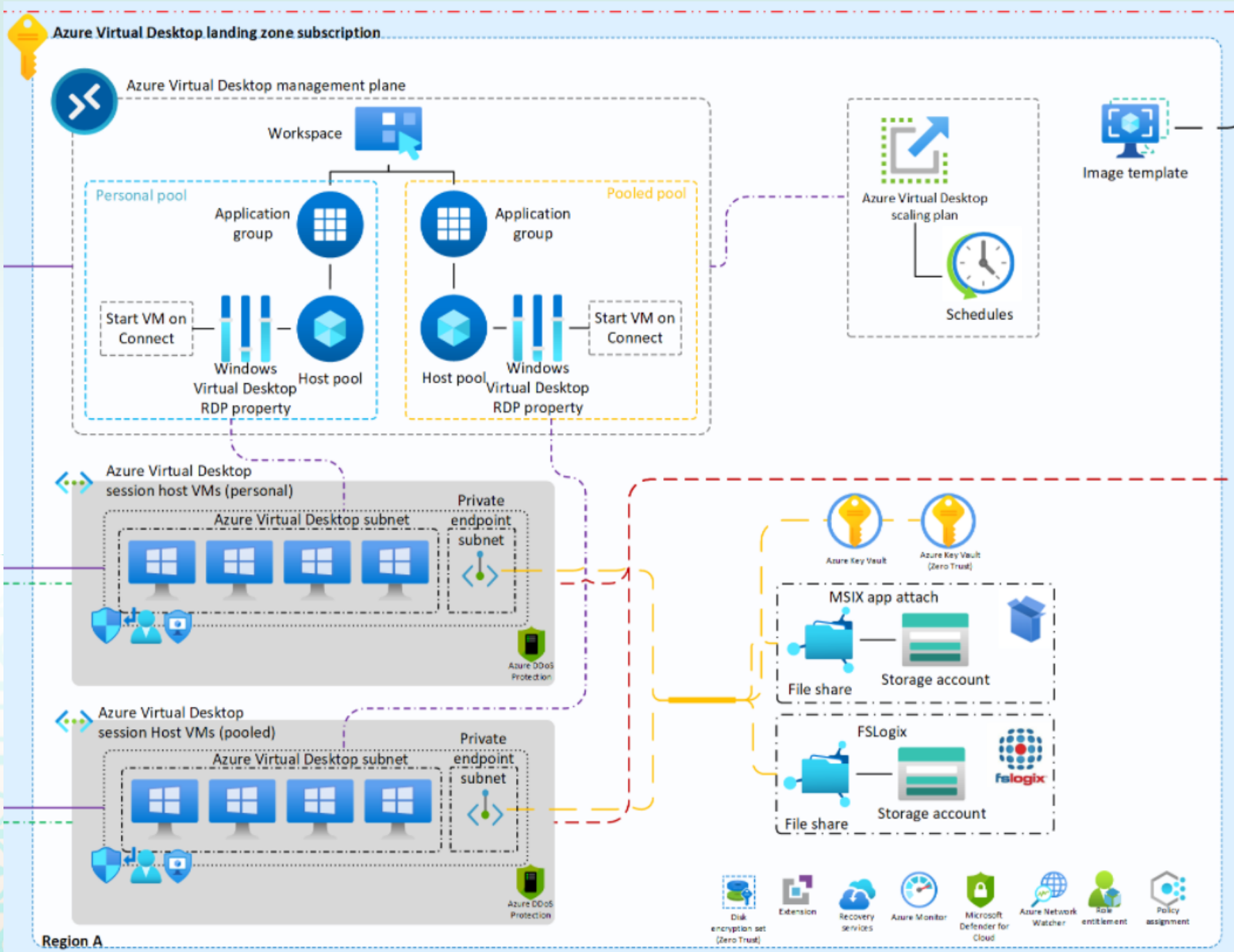
Platform Landing Zones







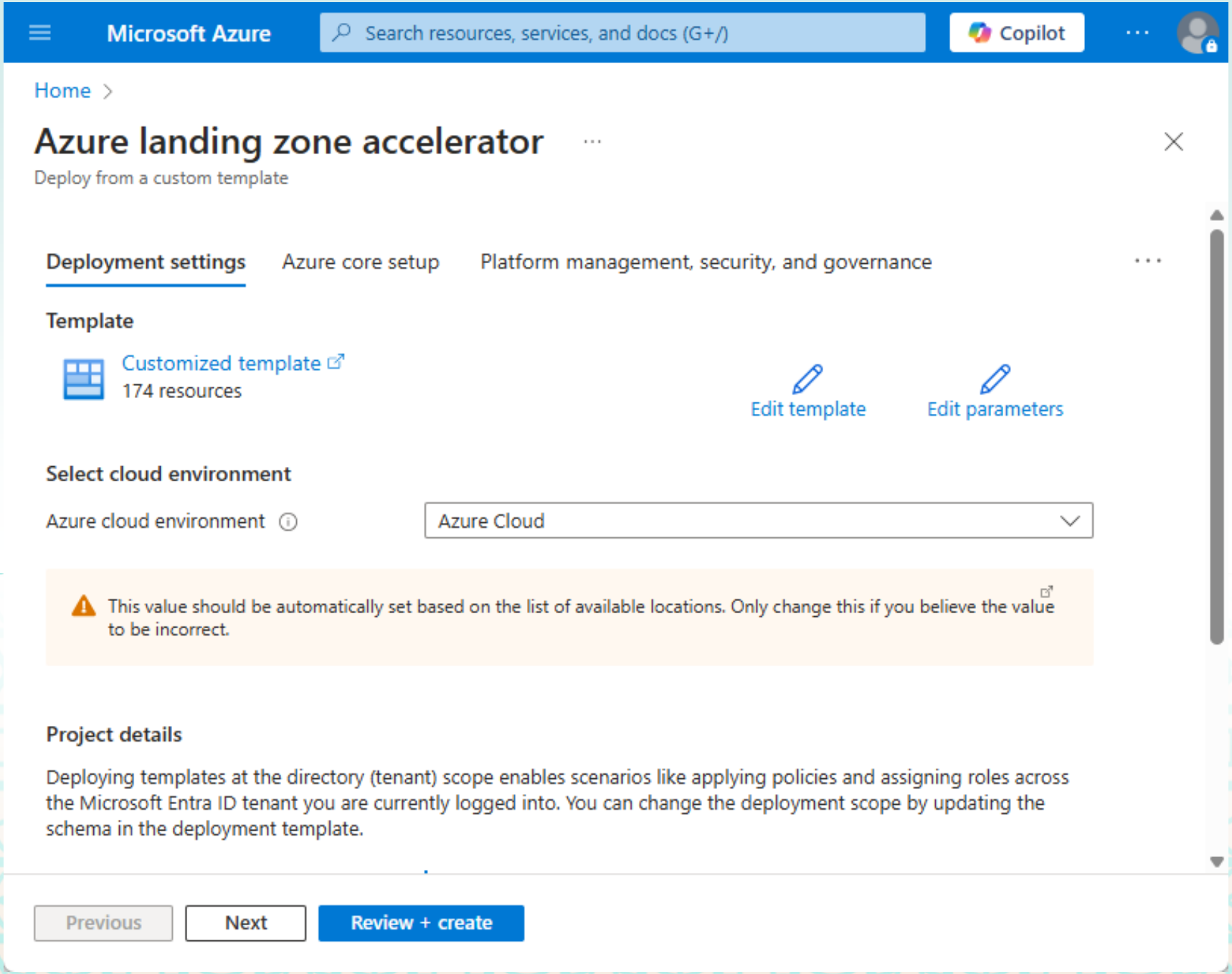
Application Landing Zone



NerdioCon 2025 PALM SPRINGS

Platform Landing Zones accelerator

Azure Platform Landing Zones accelerator



Azure landing zone accelerator

Deploy from a custom template

Template

Customized template
174 resources

Edit template | Edit parameters

Select cloud environment

Azure cloud environment: Azure Cloud

This value should be automatically set based on the list of available locations. Only change this if you believe the value to be incorrect.

Project details

Deploying templates at the directory (tenant) scope enables scenarios like applying policies and assigning roles across the Microsoft Entra ID tenant you are currently logged into. You can change the deployment scope by updating the schema in the deployment template.

Directory *: **Safari Micro Lab 1**
safarimicrolab1.com

Switching directories will result in the Azure portal being reloaded. Any progress will be lost.

Instance details

Region *: West US

Azure landing zone accelerator

Deploy from a custom template

Deploy Microsoft Sentinel (configuration required to activate)
- (•) Yes (recommended)
- ( ) No

Management subscription

Ensure you select a subscription that is dedicated/unique for Management. Selecting the same Subscription here for Connectivity or Identity will result in a deployment failure. If you want to use a single Subscription for all platform resources, select 'Single' on the 'Azure Core Setup' blade.

Management subscription *

Filter subscriptions...

SM Lab 1 Sponsorship Sub
52f3627b-0832-4b2c-ba2b-7a6eca8e959f

SML1 Identity Sub
b2adec11-165d-487b-8c04-355d9eb0b1ce

SML1 Management Sub
08e9aea7-5b9d-4719-9c69-b27ef76ff3b2

Select which Azure Monitor solutions you w
Learn more

Deploy Change Tracking

Deploy Azure Update Manager

Deploy VM Insights
- (•) Yes (recommended)
- ( ) No

Select which Microsoft Defender for Cloud solutions you will enable.
Learn more

Deploy Microsoft Defender for Cloud and enable security monitoring for your platform and resources
- (•) Yes (recommended)
- ( ) No

Microsoft Defender for Cloud Email Contact *

Previous | Next | Review + create

Azure landing zone accelerator

Deploy from a custom template

Changes on this step may reset later selections you have made. Review all options prior to deployment.

Deploy networking topology
- (○) Hub and spoke with Azure Firewall
- (●) Hub and spoke with your own third-party NVA
- (○) Virtual WAN (Microsoft managed)
- (○) No

Deploy Azure Virtual Network Manager - PREVIEW ☐

For high availability of third-party NVAs please see the guidance: Deploy highly available NVAs

Connectivity subscription

Ensure you select a subscription that is dedicated/unique for Connectivity. Selecting the same Subscription here for Management or Identity will result in a deployment failure. If you want to use a single Subscription for all platform resources, select 'Single' on the 'Azure Core Setup' blade.

Connectivity subscription * : SM Lab 1 Sponsorship Sub

Address space (required for hub virtual network) * : 10.100.0.0/16

Region for the first networking hub * : West US

Enable DDoS Network Protection
- (●) Yes (recommended)
- (○) No

Create Private DNS Zones for Azure PaaS
- (●) Yes (recommended)

Previous | Next | Review + create

Azure landing zone accelerator

Deploy from a custom template

To enable identity (AuthN/AuthZ) for workloads in landing zones, you must allocate an identity Subscription that is dedicated to host your Active Directory domain controllers. Please note, this Subscription will be moved to the identity Management Group, and ARM will assign the selected policies. We recommend using a new Subscription with no existing resources.

Assign recommended policies to govern identity and domain controllers
- (•) Yes (recommended)
- ( ) No

Identity subscription

Ensure you select a subscription that is dedicated/unique for Identity. Selecting the same Subscription here for Management or Connectivity will result in a deployment failure. If you want to use a single Subscription for all platform resources, select 'Single' on the 'Azure Core Setup' blade.

Identity subscription *: SML1 Identity Sub

Select which of the the recommended policies you will assign to your identity management group.
Learn more

Prevent inbound management ports from internet
- (•) Yes (recommended)
- ( ) No

Ensure subnets are associated with NSG
- (•) Yes (recommended)
- ( ) No

Prevent usage of public IP
- (•) Yes (recommended)
- ( ) No

Management groups

Safari Micro Lab 1

Create | Add subscription | Refresh | Expand / Collapse all | Export to CSV | Feedback

Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

Search by name or ID

Showing 4 subscriptions in 11 groups

Name	Type	ID	Total subscriptions
SM Lab 1 Sponsorship Sub	Subscription	52f3627b-0832-4b2c-ba2b-7a6eca8e959f	
sml1	Management group	sml1	3
sml1-decommissioned	Management group	sml1-decommissioned	0
sml1-landingzones	Management group	sml1-landingzones	0
sml1-platform	Management group	sml1-platform	3
sml1-connectivity	Management group	sml1-connectivity	1
SML1 Connectivity Sub	Subscription	1121fe36-5567-478f-856a-d3e518538676	
sml1-identity	Management group	sml1-identity	1
SML1 Identity Sub	Subscription	b2adec11-165d-487b-8c04-355d9eb0b1ce	
sml1-management	Management group	sml1-management	1
SML1 Management Sub	Subscription	08e9aea7-5b9d-4719-9c69-b27ef76ff3b2	
sml1-sandboxes	Management group	sml1-sandboxes	0

Policy | Compliance

Search
Overview
Getting started
Compliance
Remediation
Events
Authoring

Assign policy | Assign initiative | Refresh

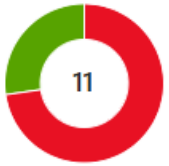
Search

Filter by name or ID...

Scope : **sml1-identity** | Definition type : **All definition types** | Compliance state : **All compliance states**

Overall resource compliance
27%
3 out of 11

Resources by compliance state



Non-compliant initiatives
4
out of 26

Non-compliant policies
16
out of 577

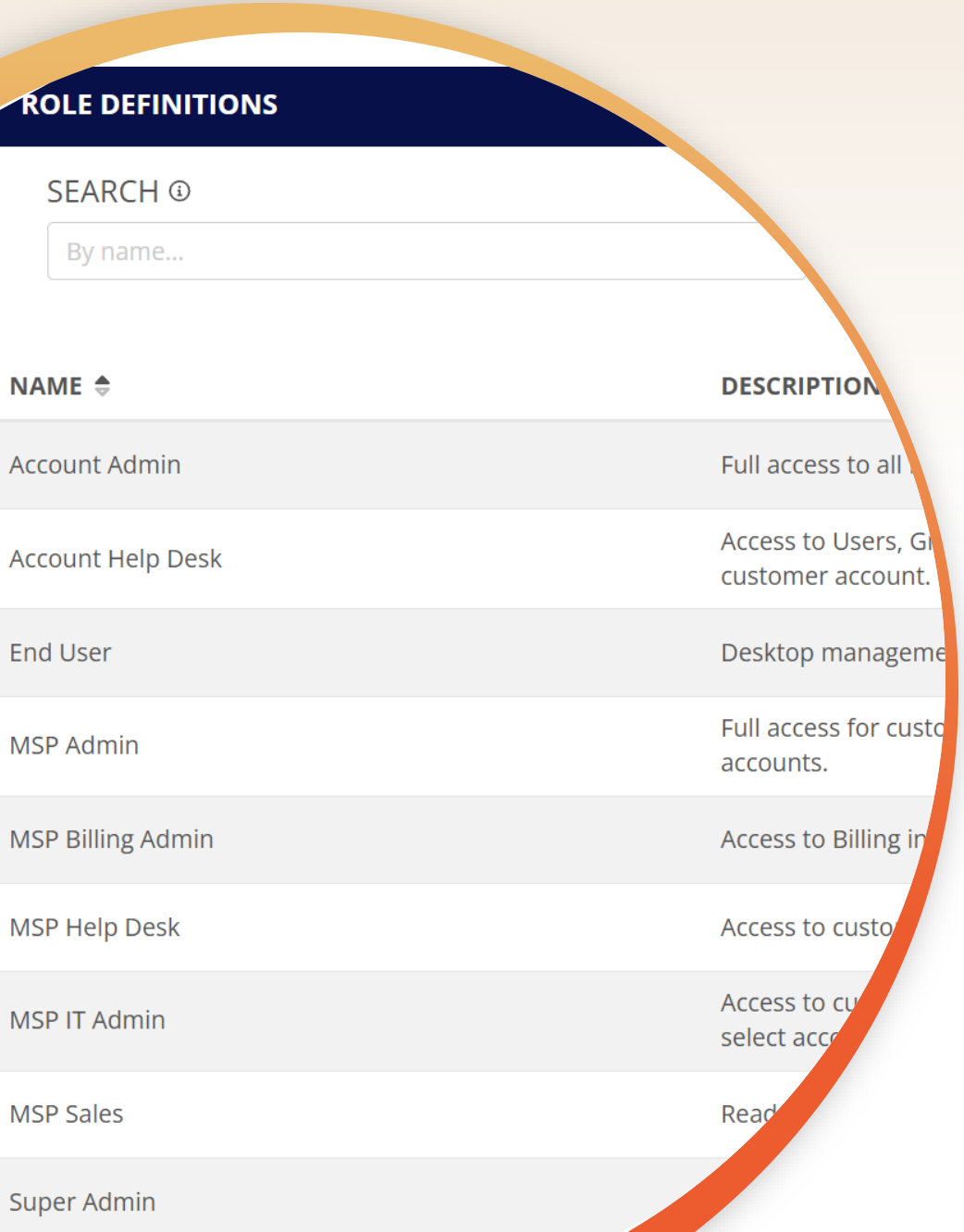
Edit columns

Name	Scope	Compliance state	Resource compliance	Non-compliant resou...	Non-compliant polici...
Microsoft Cloud Security Benchmark	sml1	Non-compliant	38% (3 out of 8)	5	2
Subnets should be private	sml1-platform	Non-compliant	0% (0 out of 2)	2	1
Deploy Microsoft Defender for Cloud confi	sml1	Non-compliant	0% (0 out of 1)	1	3
Resource Group and Resource locations sh	sml1	Non-compliant	80% (4 out of 5)	1	1
Deploy Azure Monitor Baseline Alerts - No	sml1	Non-compliant	0% (0 out of 1)	1	2
Deploy Azure Monitor Baseline Alerts for S	sml1	Non-compliant	0% (0 out of 1)	1	6
Configure Azure Activity logs to stream to	sml1	Non-compliant	0% (0 out of 1)	1	1
Configure multiple Microsoft Defender for	sml1	Compliant	100% (1 out of 1)	0	0
Enable category group resource logging fc	sml1	Compliant	100% (2 out of 2)	0	0
Subnets should have a Network Security G	sml1-identity	Compliant	100% (2 out of 2)	0	0
Configure backup on virtual machines with	sml1-identity	Compliant	100% (0 out of 0)	0	0
Management port access from the Internet	sml1-identity	Compliant	100% (0 out of 0)	0	0

Using NMM in AVD Well-Architected Framework with Landing Zones

Before we get started: Need to know

- Bringing Landing Zones into NMM will require a high level of Nerdio + Azure knowledge
- Using the accelerator will get a create a solid foundation
- The accelerator can cause some issues with NMM deployments
- Mix of resources created by NMM, created in NMM, and created in Azure



Prepping Nerdio Manager

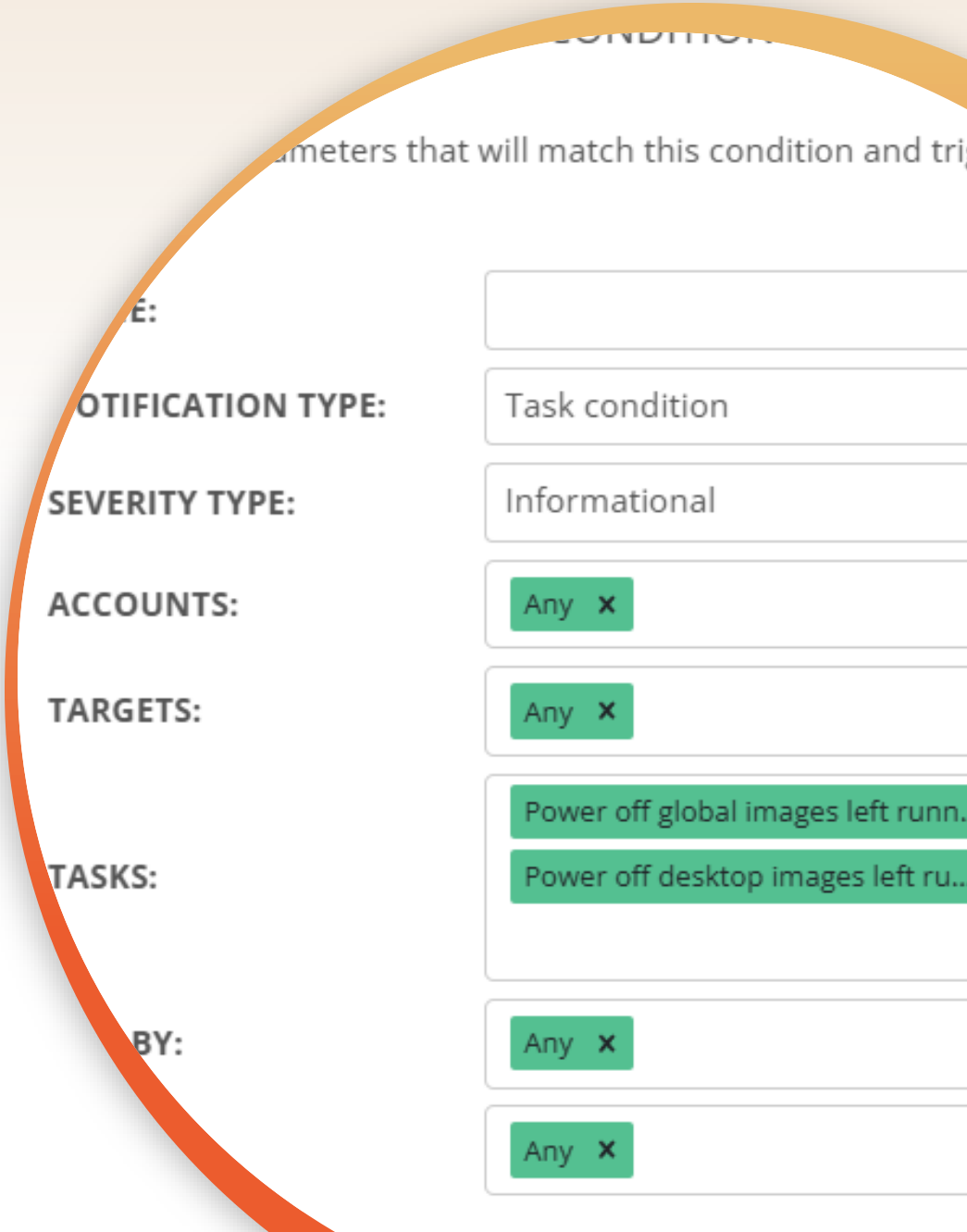
Users and roles

- Define your roles
  - Nerdio Manager comes with pre-made roles
  - Think internally how your team operates
- Assigning roles in Nerdio Manager
  - Save time copying from existing roles
  - Create security groups within your MSP tenant for each role
    - No direct assignments!
- Setup workflows
  - Require approval step for actions you define
  - Extra layer of protection for sensitive actions
- Setup group templates + conditional access
  - Deploy and report on policies at scale

Prepping Nerdio Manager

Notifications and alerting

- Proactive alerting for performance and cost issues
- Pre-canned notification conditions
- Recommended notification conditions
  - Usage conditions
    - CPU, RAM, OS disk queue
  - Backup conditions
  - Defender for Endpoint conditions
  - Reservation conditions
  - Task conditions
    - Images left running
    - Auto-scale alerts
    - Start./Host alerts
- Setup Email/PSA integration
  - Azure Communication Services on by default

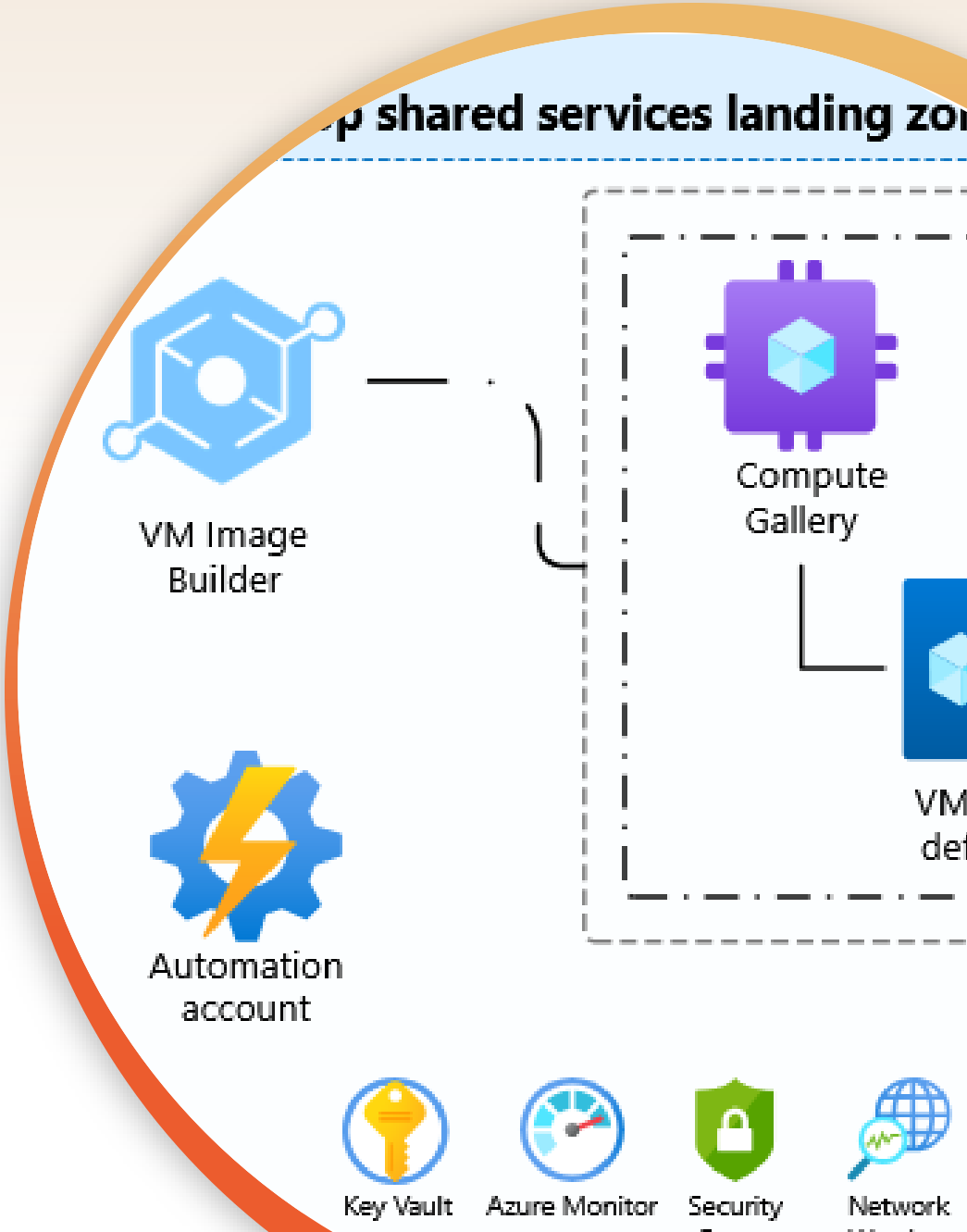


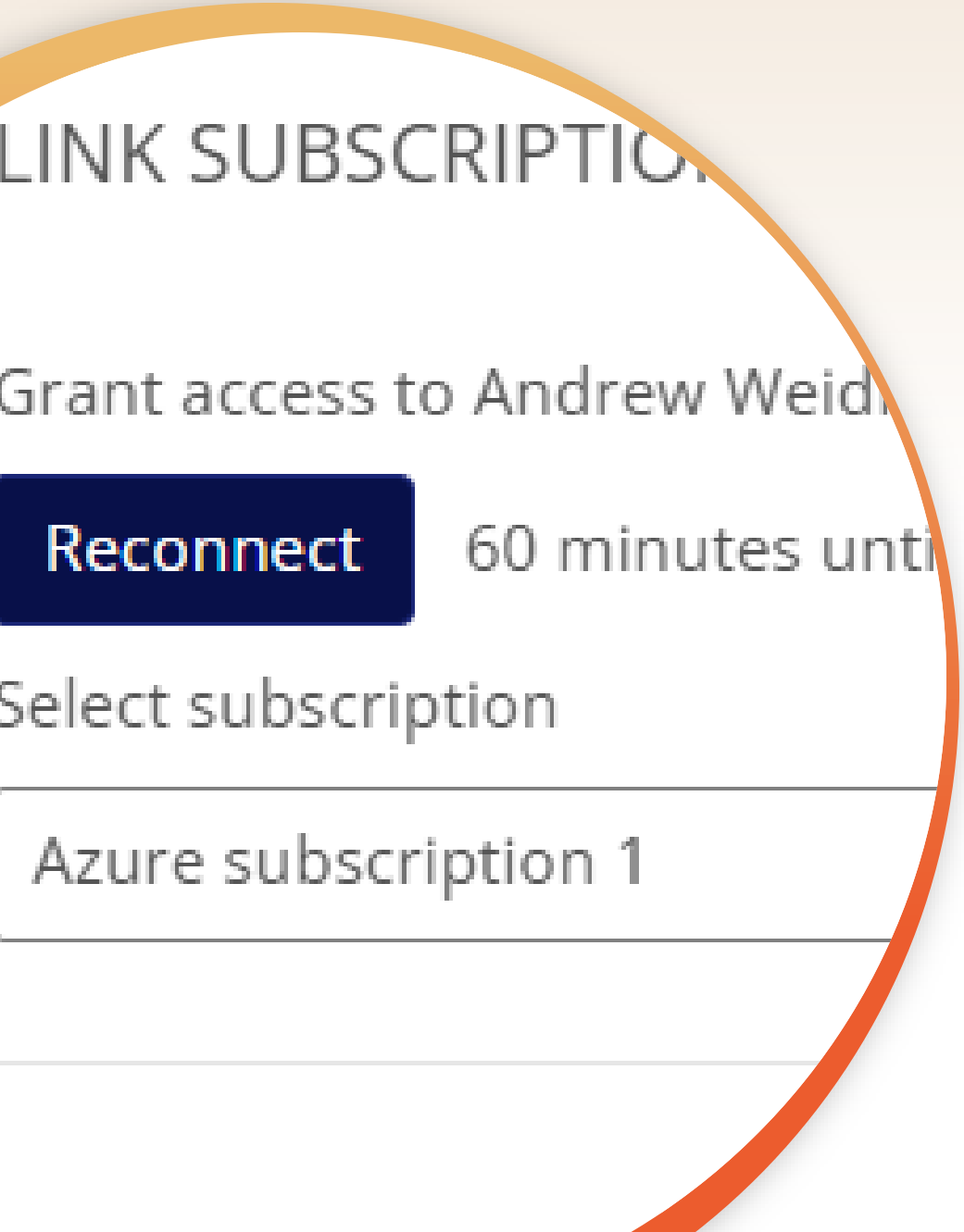
Connecting an account

1. Ensure you have used the accelerator before trying to connect.
2. Additional subscriptions: Application Landing Zones
    - Virtual Desktop Shared Services
    - AVD Landing Zone
3. Add an account
    - Utilize partner center integration
    - Manual account add
        - Choose Modern Work and Entra ID

Linking first subscription

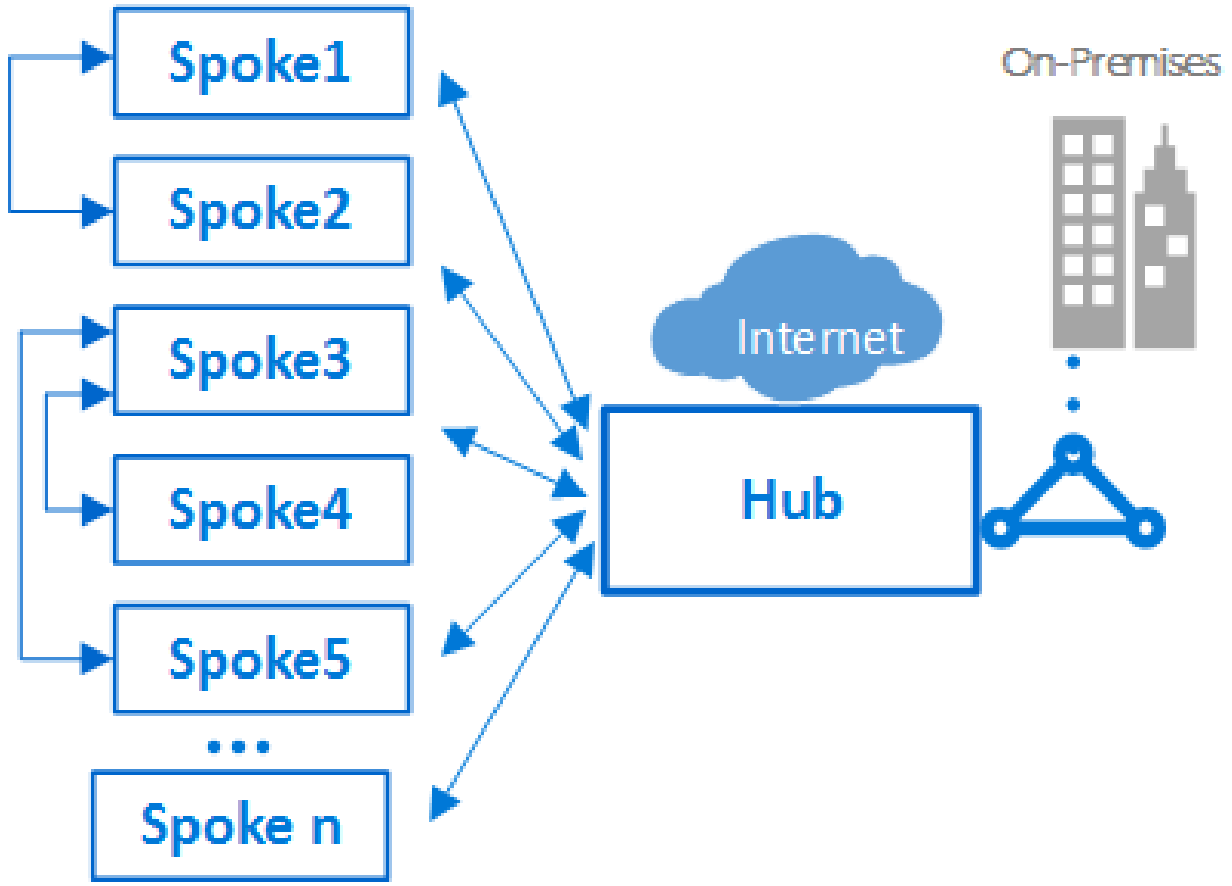
1. First sub to link: **Virtual Desktop Shared Services**
    - Setup backend AVD infrastructure
2. Link resource group
    - Main shared services resource group
    - Remember to make default
3. Create key vault
4. Create automation account
    - Enable Azure Runbook Scripted Actions
5. Enable Azure Virtual Desktop
    - Settings > Integrations > Desktop Deployment Model





Adding additional subscriptions

1. Link connectivity subscription
2. Link management subscription
    - This is a platform subscription, but Nerdio currently doesn't use most of this
3. Link Azure Virtual Desktop Landing Zone(s) subscription
4. Link identity subscription
    - ADDS
    - Entra Domain Services


Spoke1
Spoke2
Spoke3
Spoke4
Spoke5
...
Spoke n
Internet
Hub
On-Premises

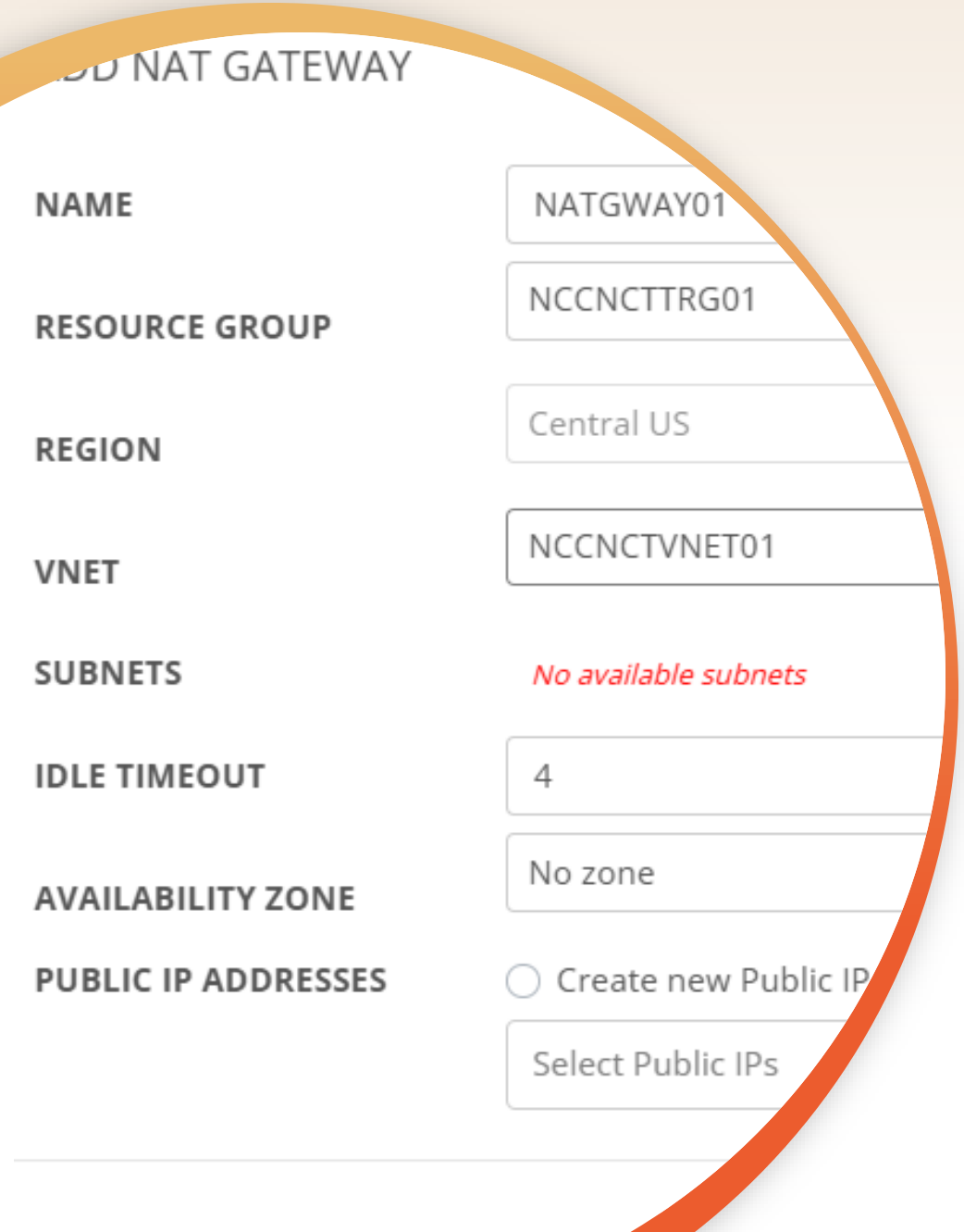
Networking

Within Nerdio Manager

- Vnet
- VPN
- NSG
- NAT Gateway
- Peerings

Within Azure

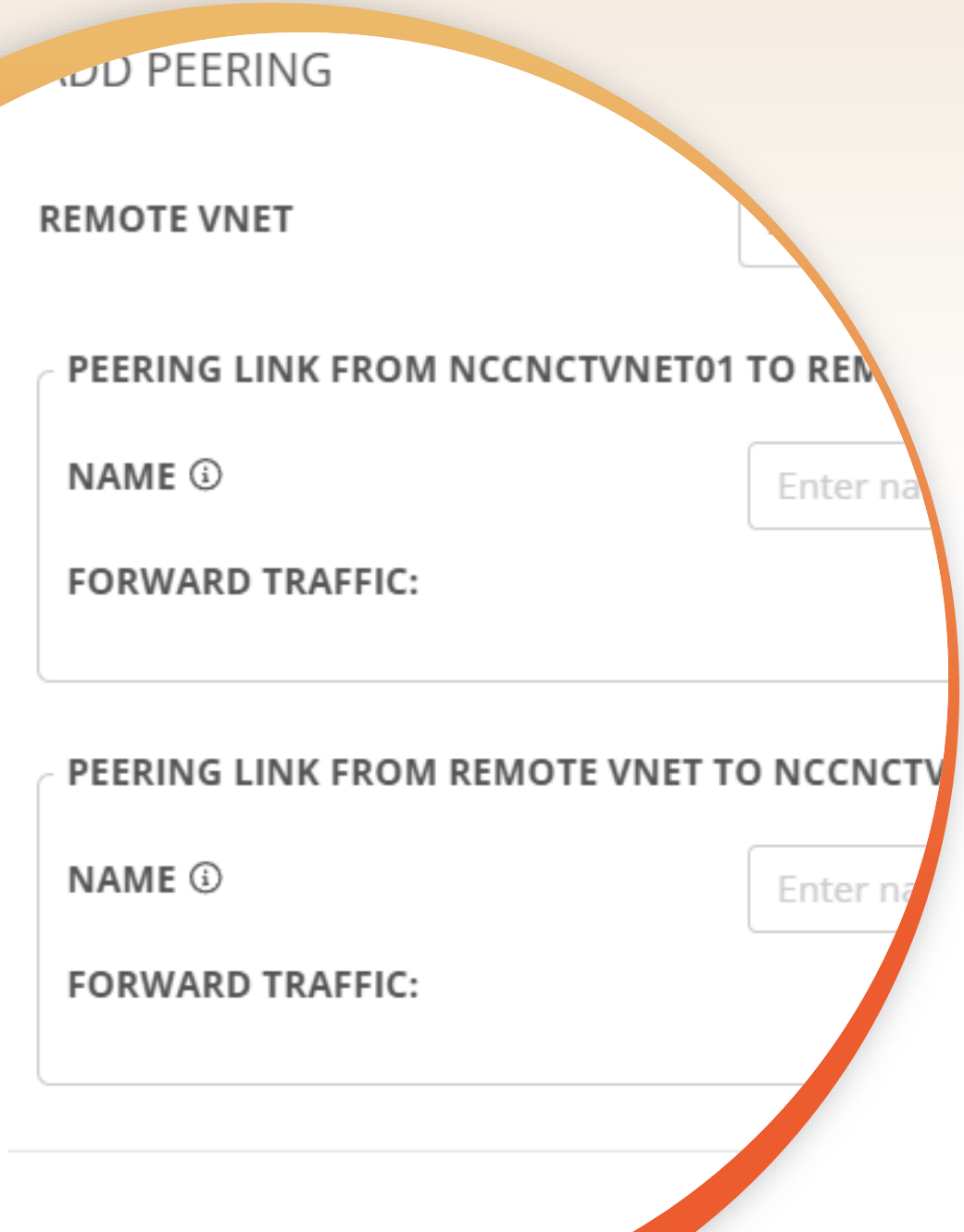
- Azure Firewall/NVAs
- Express Route
- Private Endpoints



Outbound access setup

Within Nerdio Manager

1. **Create outbound access VNet/Subnet**
2. **Add NAT Gateway**
   - Use previous VNet/Subnet
   - Keep in mind Availability Zone
   - Public IP
3. **DNS Servers**
   - Own subnet, with NSG



Linking it all together

1. **Use VNET Peering to link the VNETs together**
    1. Outbound Connectivity
    2. AVD Shared Services
    3. AVD Landing Zones
    4. Identity
2. **Private Link**
    1. Link Azure PAAS resources to your VNETs
        1. FSLogix and App Attach to Virtual Desktop
    2. Not officially supported (yet)

What's left?

Virtual Desktop Shared Services

- Create Azure Compute Gallery
- Create Desktop Images
- Setup scripts and application management

AVD Landing Zone

- Create AVD Workspace
- Create your host pools
- Monitoring
- Auto-scaling/AS Profiles

Identity

- Create Domain Controllers
- Entra Domain Services

The future of Nerdio Manager for MSP and Landing Zones

- Plan to work towards utilizing Well-Architected Framework by default
- Default deployments use a simplified Landing Zone architecture
- New "advanced" add an account experience to support full blown WAF deployments
- Hub-and-spoke networking
- What else?

More WAF & ALZ Content at MS Cloud Bros blog & YouTube channel

mscloudbros.com

Youtube.com/@mscloudbros