



Microsoft Azure Foundations for CSP partners

Jan Depping PTS
Herman Keijzer PDM

SPEAKERS



Jan Depping

**Senior Partner Technology
Strategist**



Herman Keijzer

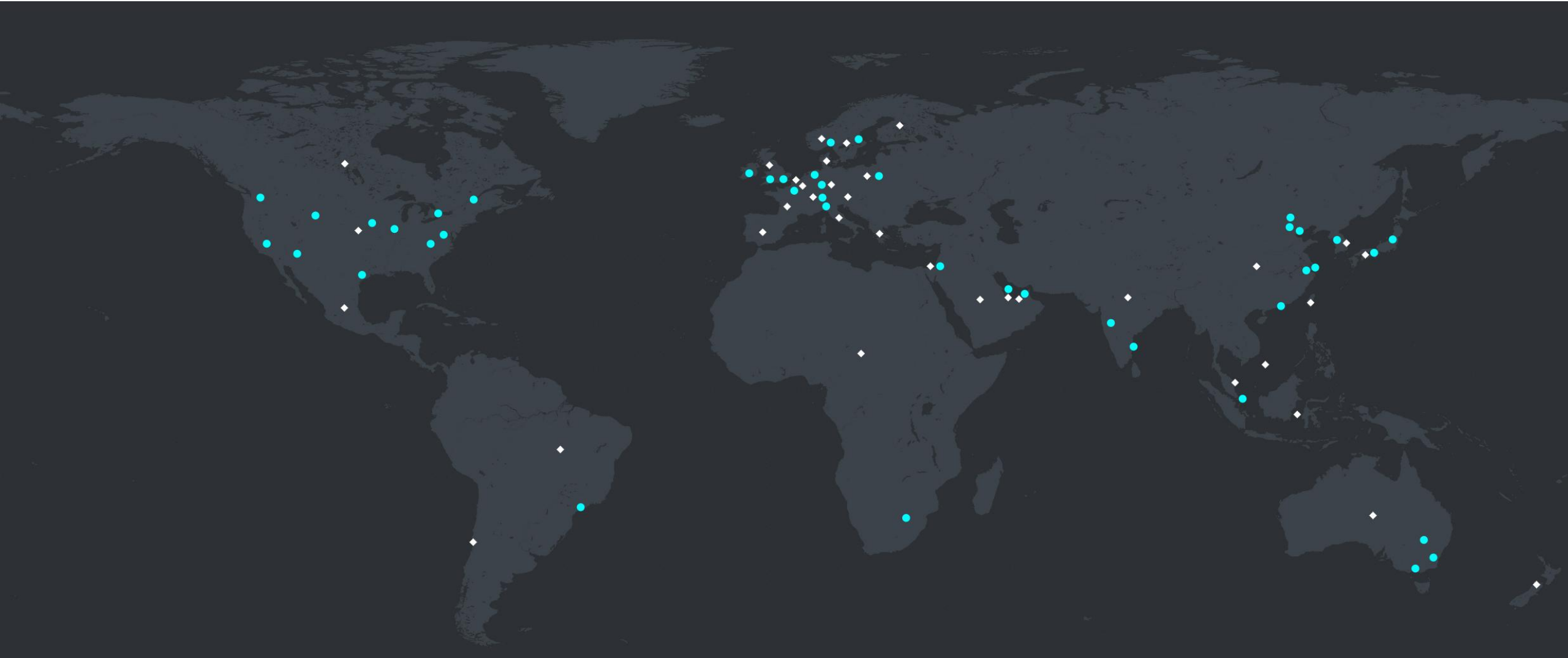
**Hoster Partner
Development Manager**

Agenda

-
- Azure Concepts & Terminology
 - Azure foundations
 - Maintaining environment in Azure
 - Extra
 - Landing zones
 - Zero Trust (governance/security)

Azure Concepts & Terminology

Azure Geographies & Regions

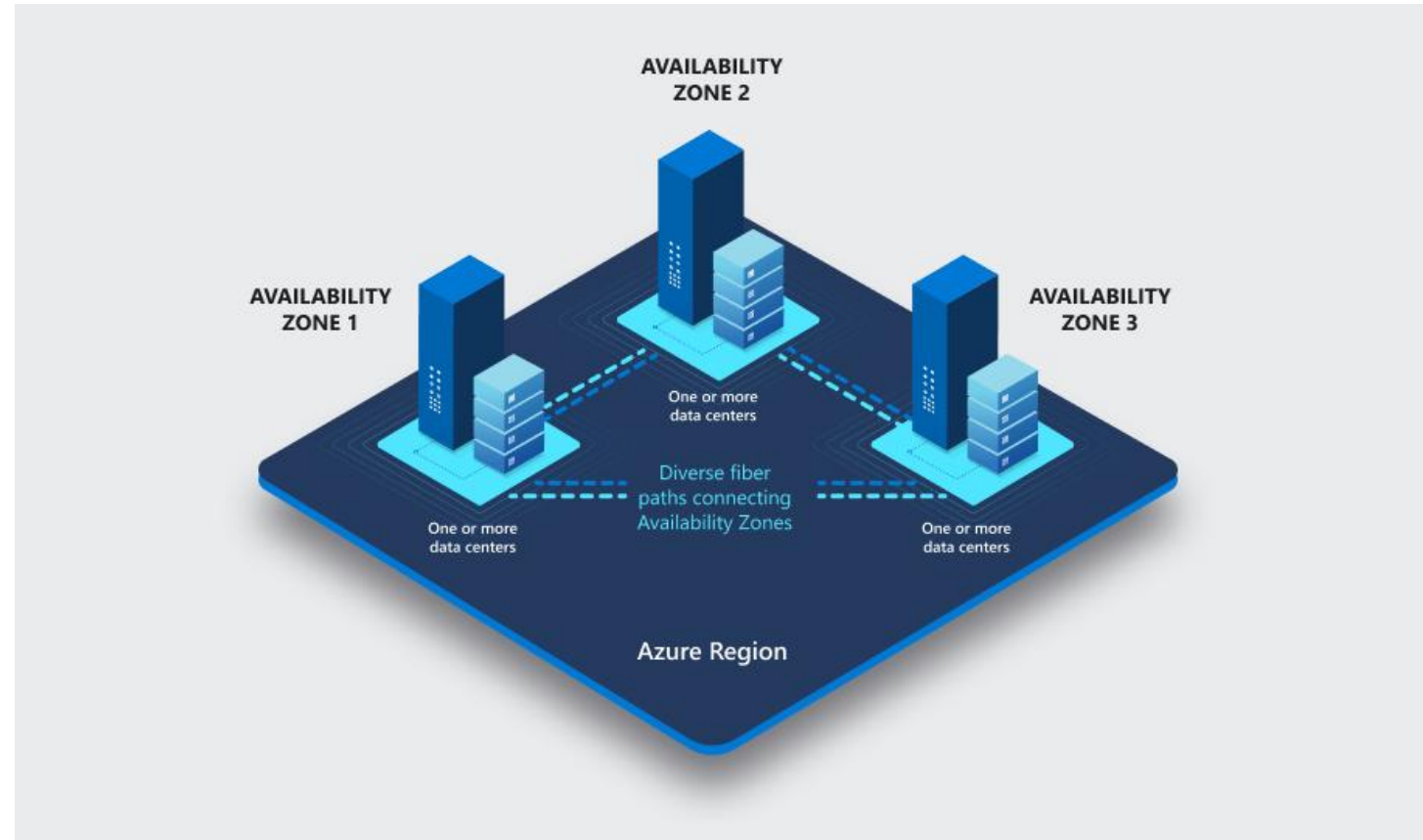


Netherlands (region: "West Europe")



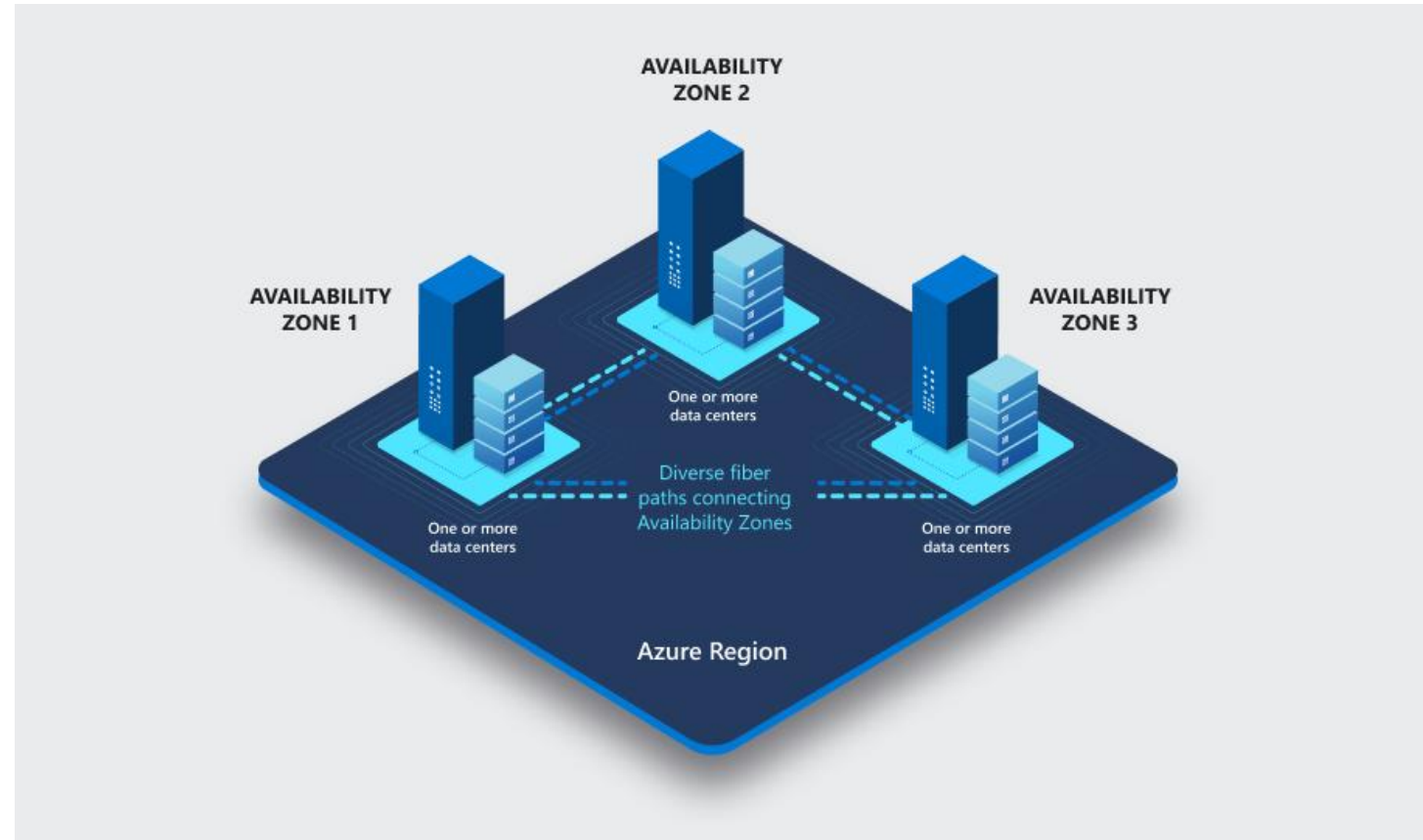
Azure Regions

- Datacenters are grouped into geographic regions
- Multiple datacenters within each region
- Resources are created in defined regions like "West US", "North Europe" or "Southeast Asia"



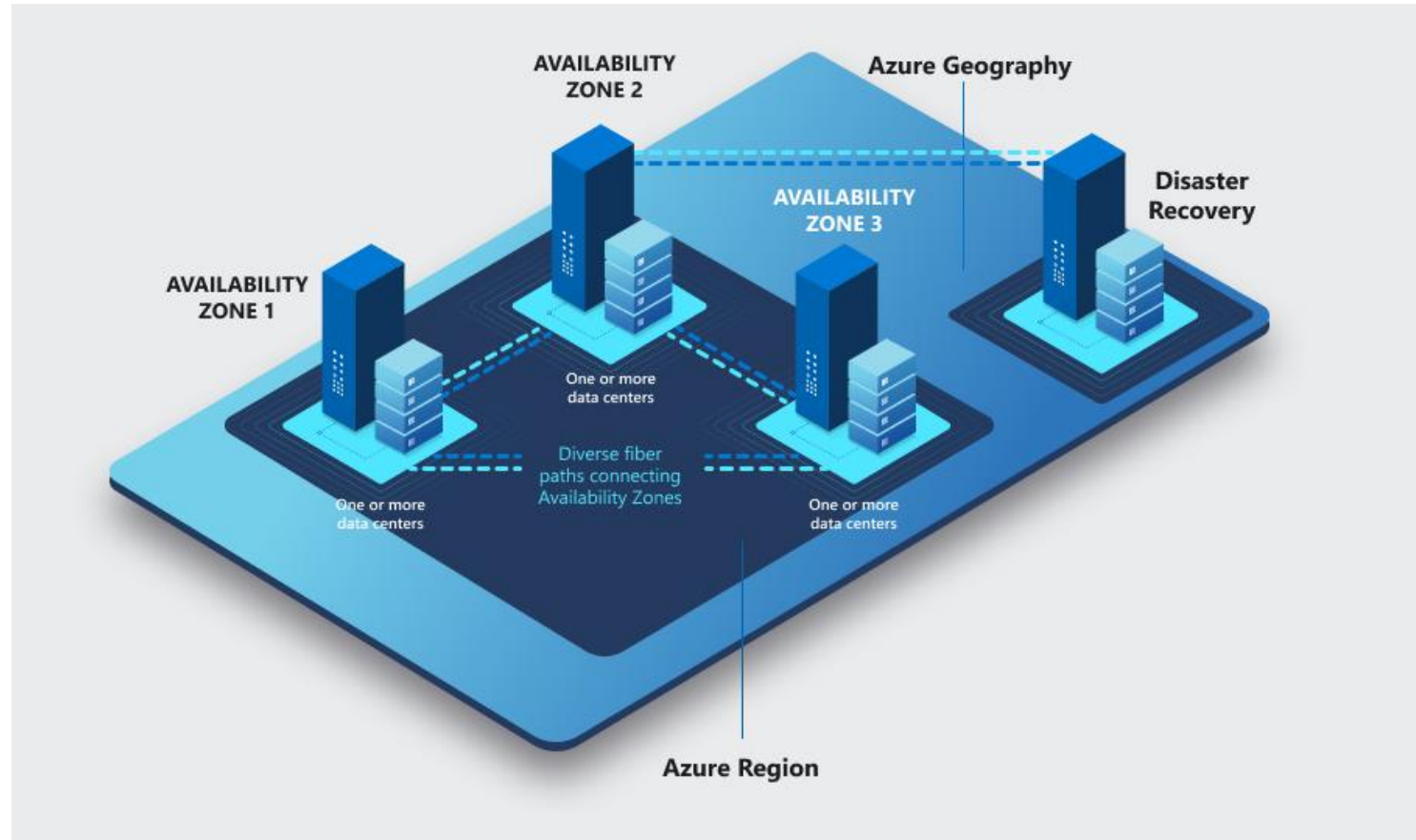
Availability Zones

- Separated groups of datacenters within a region
- Close enough to have low-latency connections to other availability zones
- Far enough apart so no more than one will be affected by outages
- Have independent power, cooling, and networking infrastructure
- Azure services that support Availability Zones fall into either Zonal services or Zone-redundant services

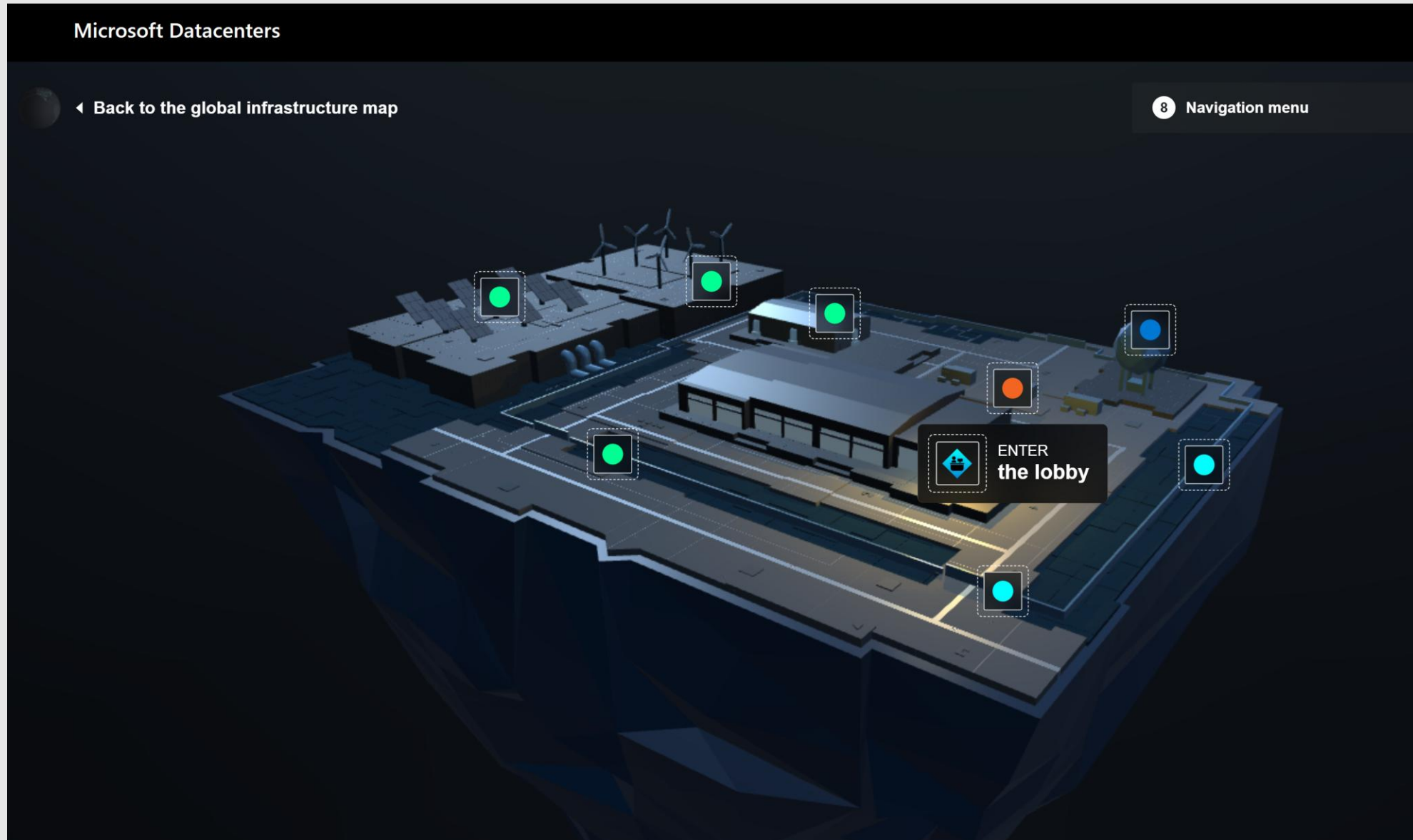


Region Pairs

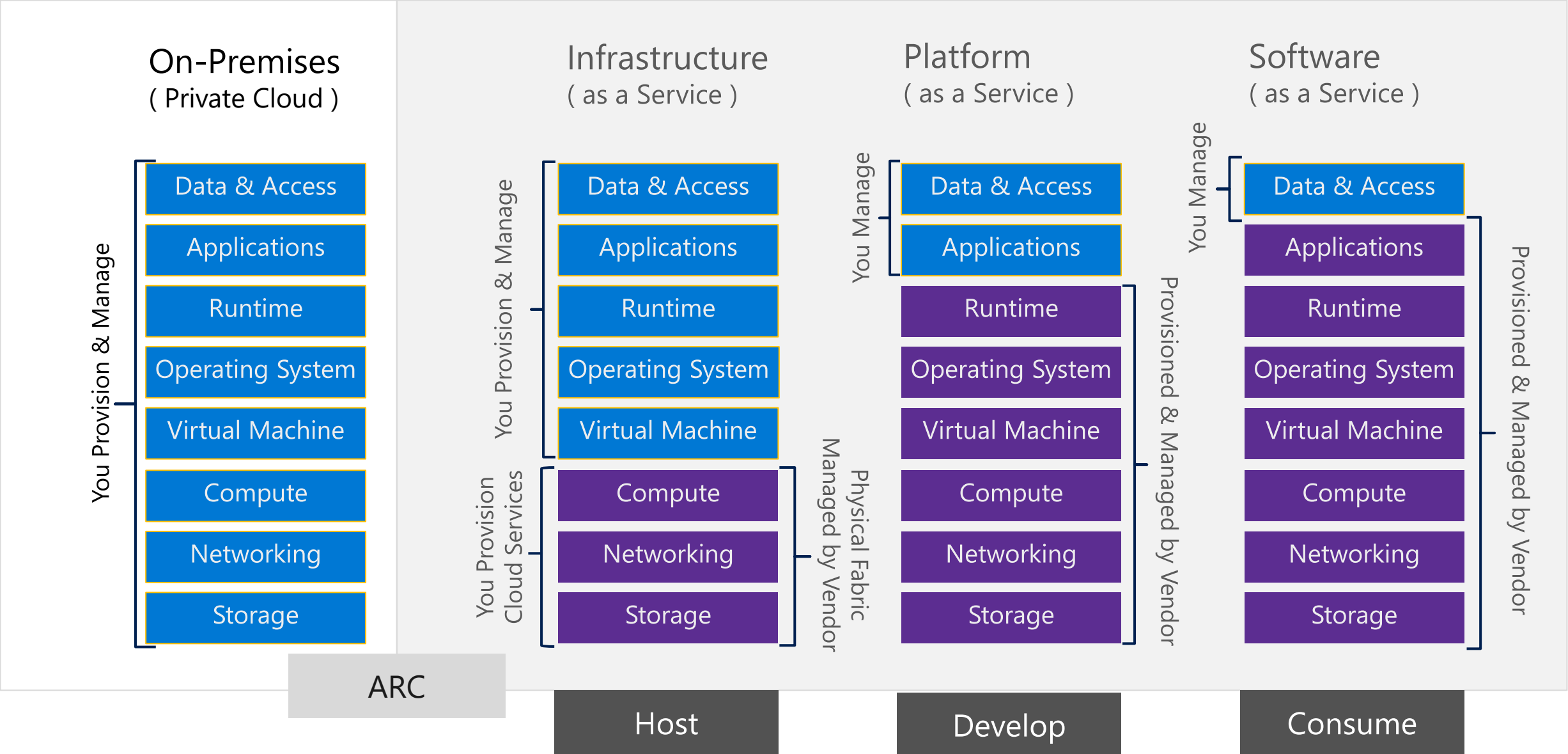
- Paired within the same geography
- Allows for the replication of resources
- Enables Disaster Recovery



[Virtual datacenter tour | Azure global infrastructure experience](#)



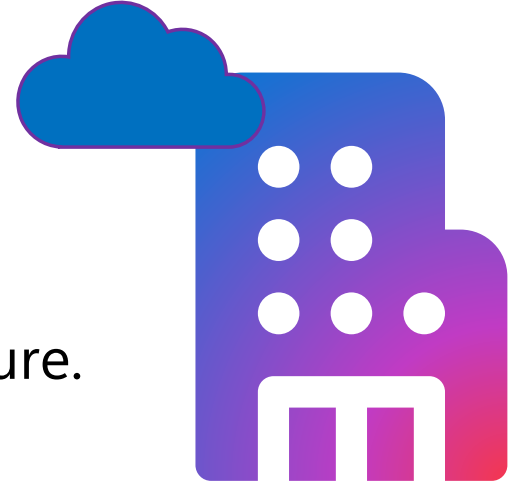
Azure Cloud Computing Capabilities



Organization

An Organization represents a business entity that is using Azure.

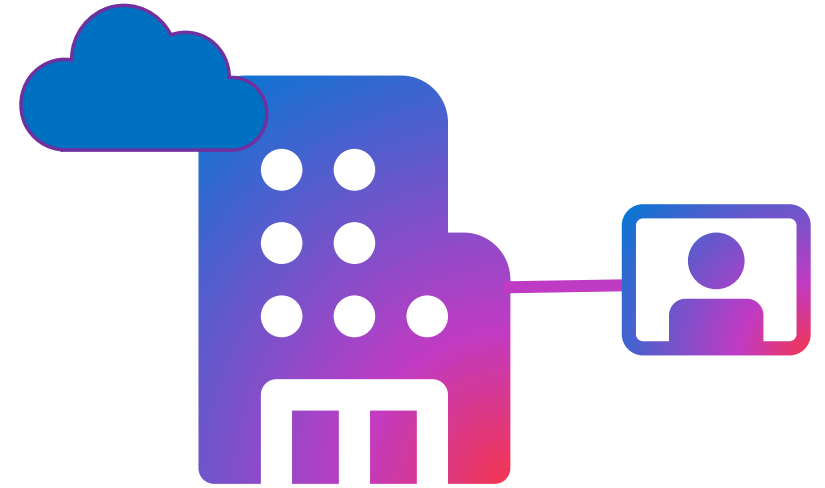
The Organization is a container for Subscriptions.



Tenant

A specific instance of Microsoft Entra ID containing user accounts and groups.

Only one Tenant is linked to an Organization to allow users access to Azure resources.



Subscriptions

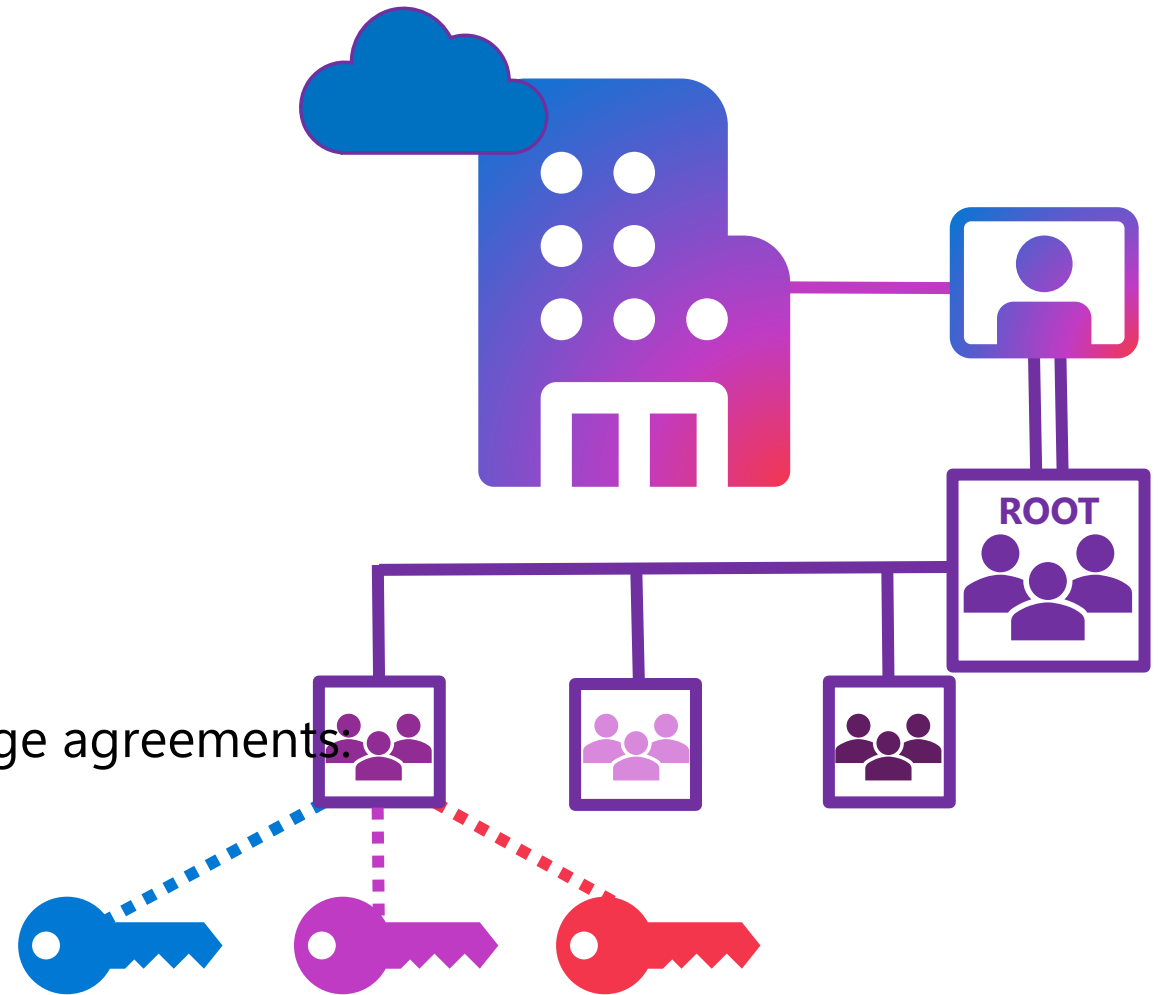
A point of billing for Azure resource consumption.
Can Be Considered A 'Security Container'

Organizations can have multiple Subscriptions.

Different types of Subscriptions offer different usage agreements:

- Free Trial
- Pay-As-You-Go
- Visual Studio Subscription
- CSP Azure plan

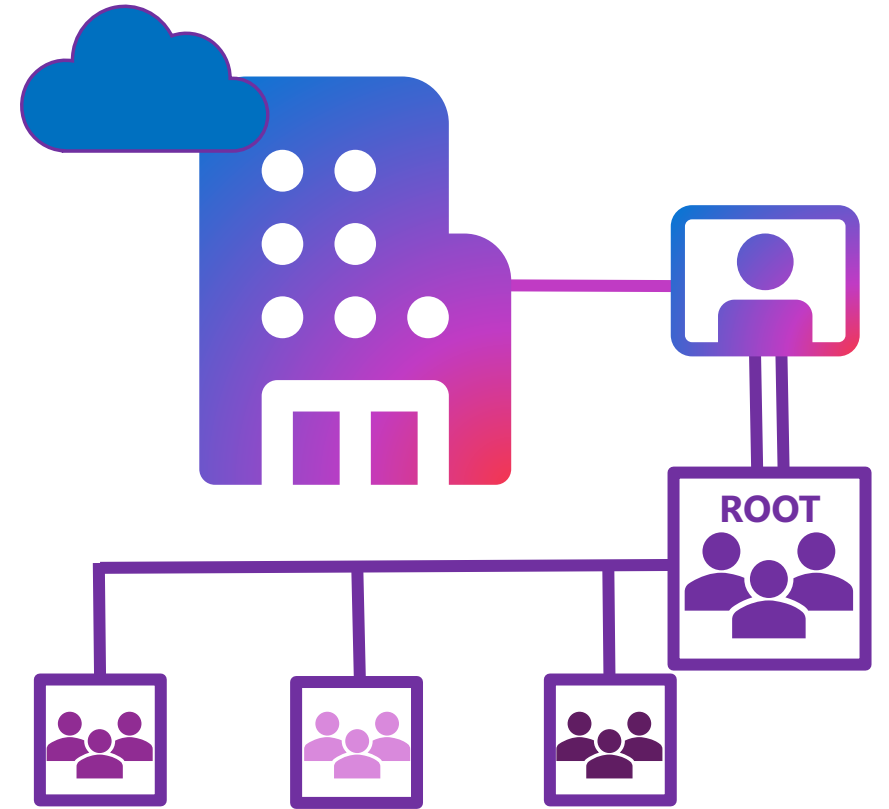
Remember; [Azure subscription and service limits, quotas, and constraints - Azure Resource Manager | Microsoft Learn](#)



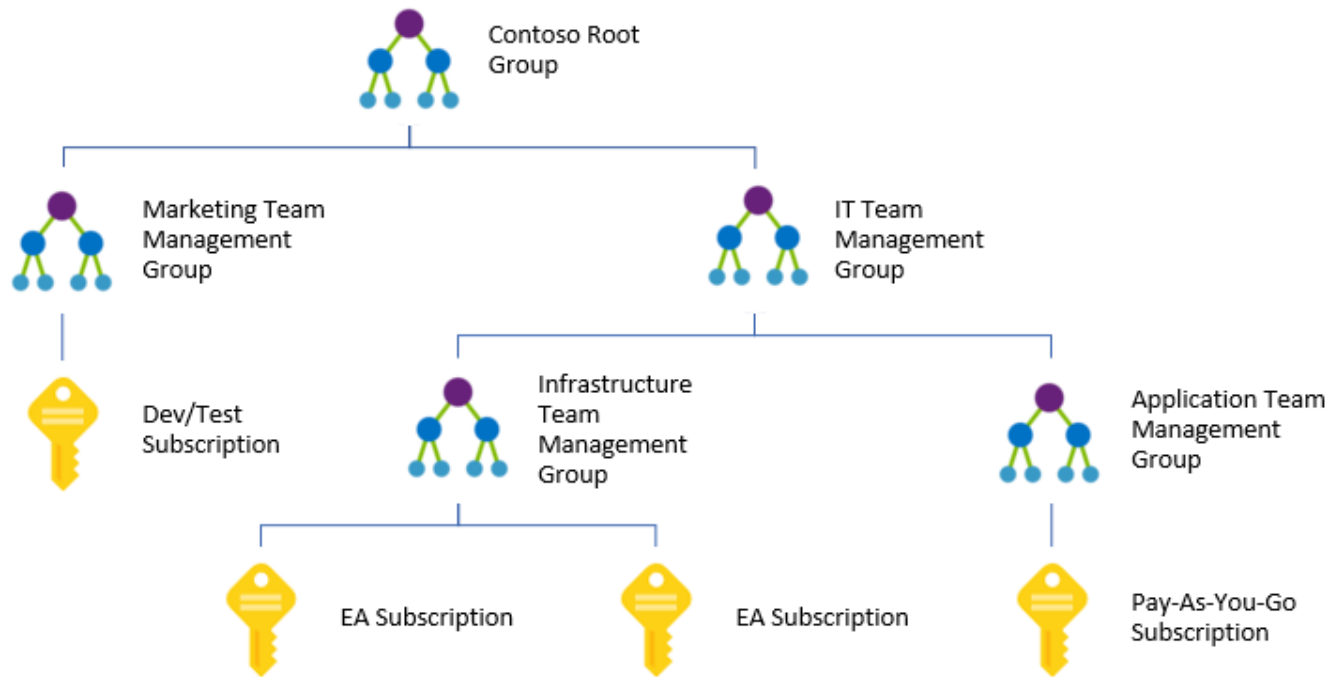
Management Groups

User-defined organizational groups which provide a governance scope to efficiently manage access, policies, and compliance across Azure subscriptions.

The Root Management Group ID is the same as the Tenant. One Tenant can support up to 10,000 Management Groups.



Management Groups to organize subscriptions



Create a custom management hierarchy to fit your organization

Enables RBAC, policies for tagging, cost analysis and budgets at any scope

Shared with Policy, Security Center, Privileged Identity Management services

Least-privileged RBAC roles



Azure RBAC Role	Description	Example Personas
Cost Management Reader	Read access to all cost mgmt. features, but no changes allowed	Azure service owner, it dev ops, finance analyst
Cost Management Contributor	In addition cost management reader can create budget and alert creation	Azure service owner, finance manager, dept. or product owner
Billing Reader	Has read-only access to billing information in Azure portal	Finance manager
Reader	Read access	
Contributor	Lets you view everything, but not make any changes	
Owner	Lets you manage everything, including access to resources	

[Azure built-in roles - Azure RBAC | Microsoft Learn](#)

1. You define what someone can do (role).
2. You define where they can do it (scope).
3. You assign that role to who needs it (user/group/app).

<<

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

All resources

Recent

App Services

Virtual machines (classic)

Virtual machines

SQL databases

Cloud services (classic)

Subscriptions

Microsoft Entra ID

Monitor

Microsoft Defender for Cloud

Help + support

Advisor

Cost Management + Billing

Home > Resource groups > arc | Access control (IAM) >

Add role assignment ...

Role

Members

Conditions

Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles

Privileged administrator roles

Grant privileged administrator access, such as the ability to assign roles to other users.

Can a job function role with less access be used instead?

Search by role name, description, permission, or ID

Type : All

Category : All

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to assign roles i...	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign rol...	BuiltInRole	General	View
Access Review Operator Servic...	Lets you grant Access Review System app permissions to discover and revoke a...	BuiltInRole	None	View
Azure File Sync Administrator	Provides full access to manage all Azure File Sync (Storage Sync Service) resourc...	BuiltInRole	None	View
Role Based Access Control Ad...	Manage access to Azure resources by assigning roles using Azure RBAC. This ro...	BuiltInRole	None	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General	View

Showing 1 - 6 of 6 results.

Review + assign

Previous

Next

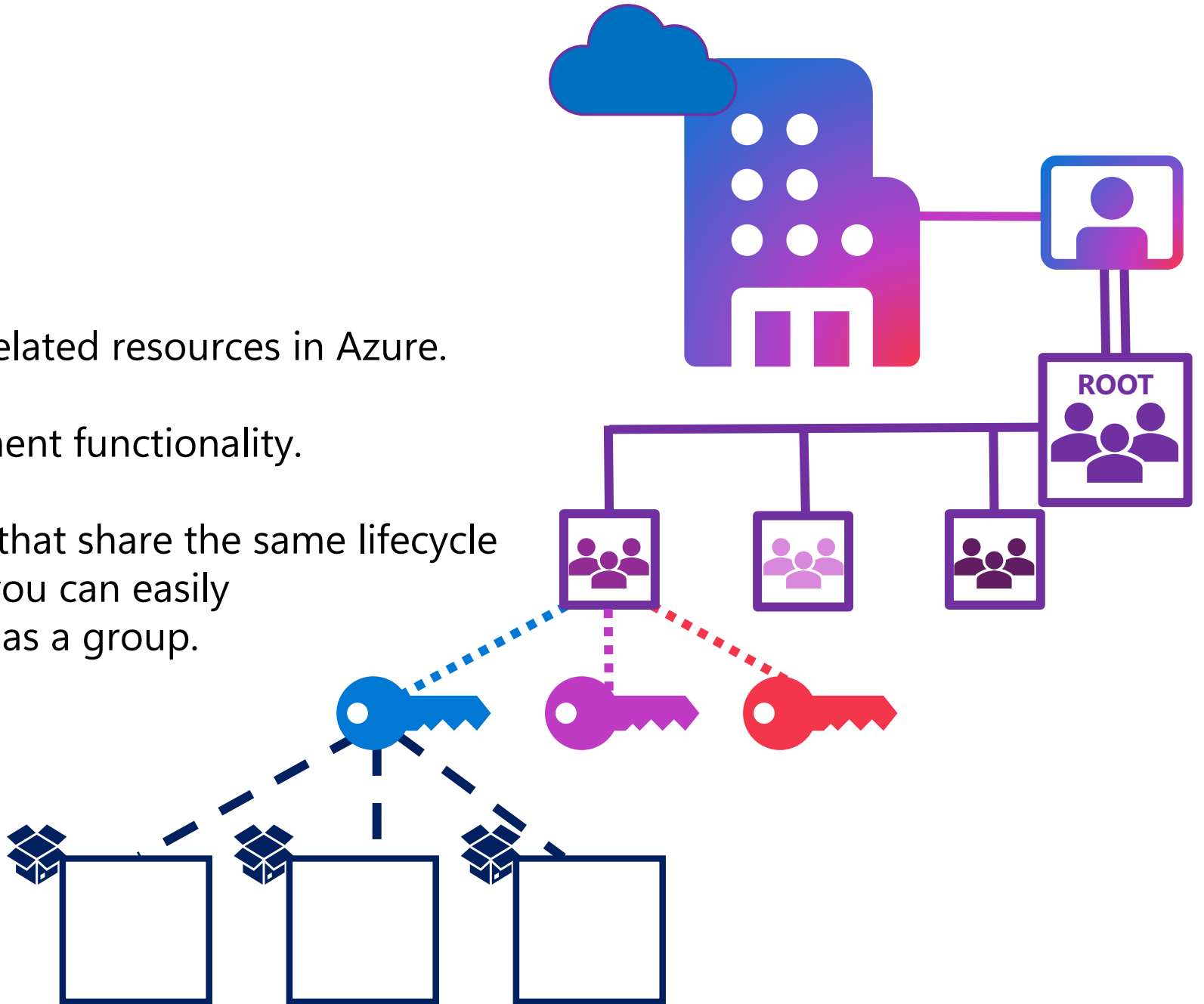
[Assign Azure roles using the Azure portal - Azure RBAC | Microsoft Learn](#)

Resource Groups

An organizational container for related resources in Azure.

Provides bulk resource management functionality.

Best practice is to add resources that share the same lifecycle to the same Resource Group so you can easily deploy, update, and delete them as a group.



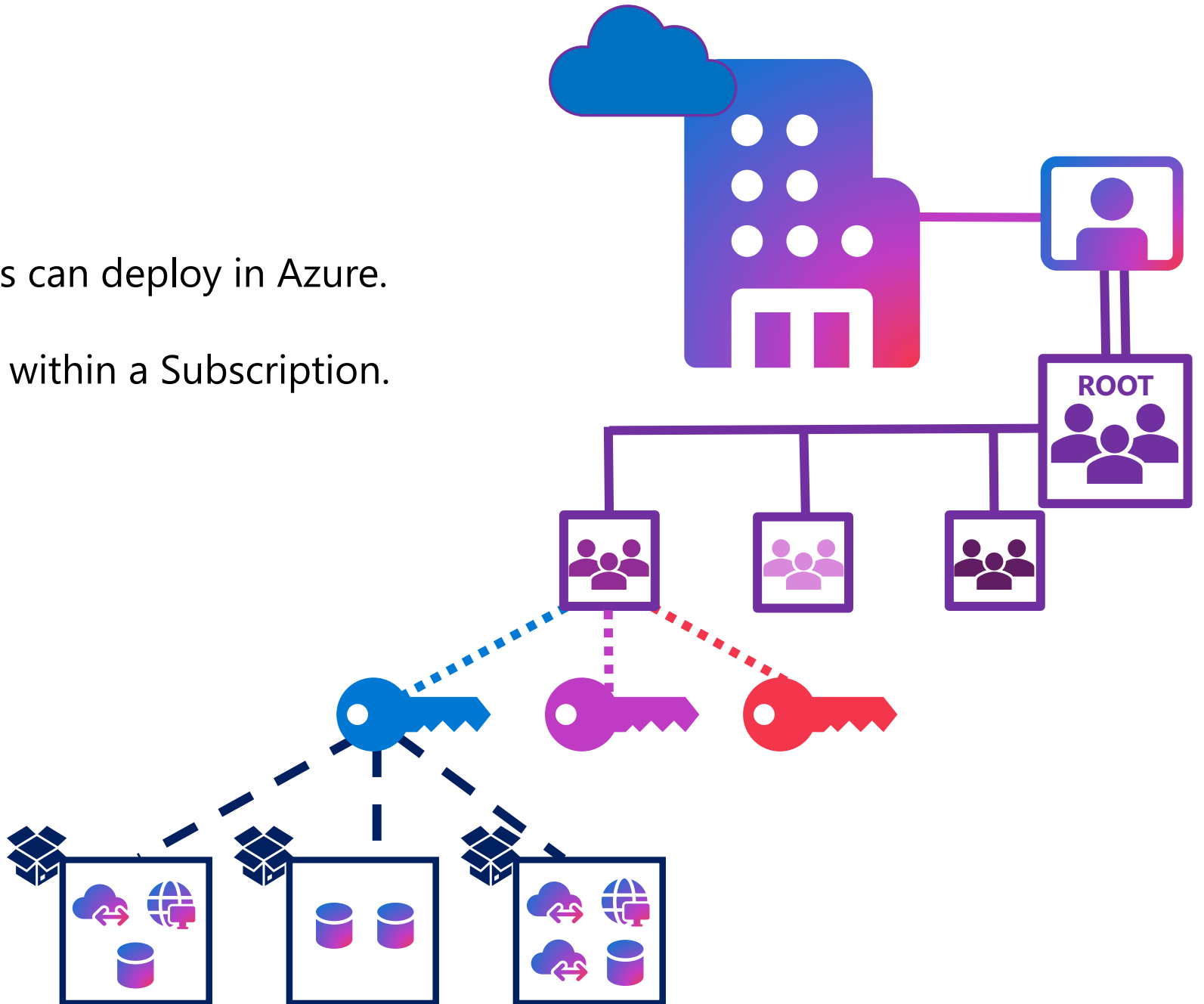
Resources

A service or technology that users can deploy in Azure.

Exists inside one Resource Group within a Subscription.

Examples of resources:

- Virtual Machines
- Managed Disks
- Virtual Networks
- Network Security Group
- Storage Accounts
- Load Balancer
- Key Vault
- And much, much more...

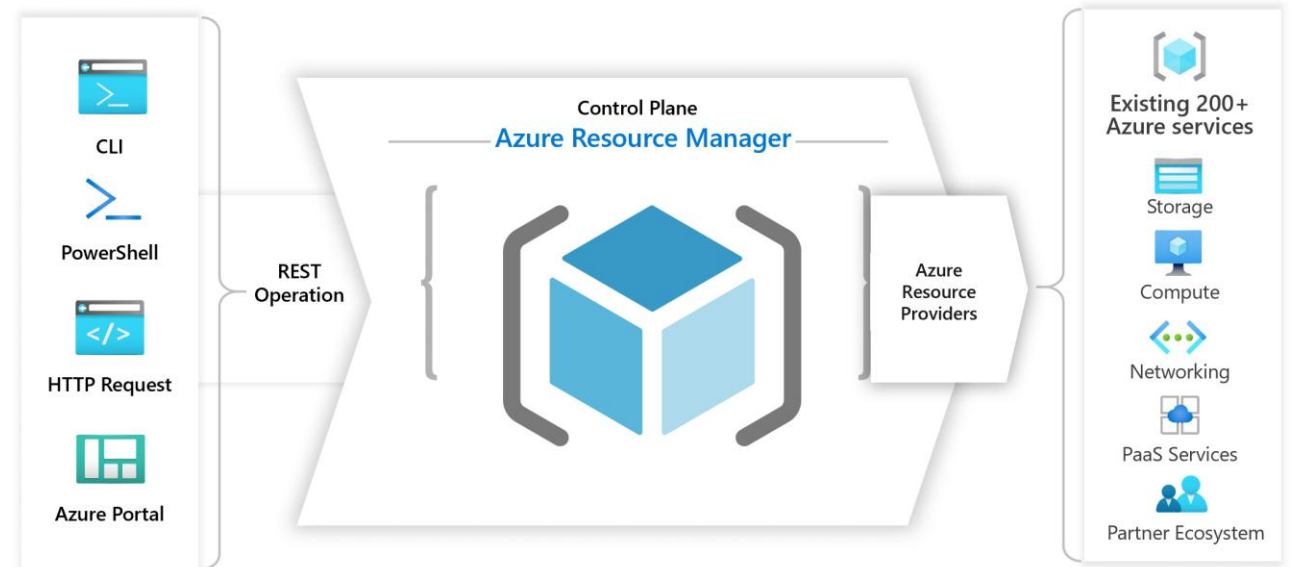




Azure foundation

Azure Resource Manager

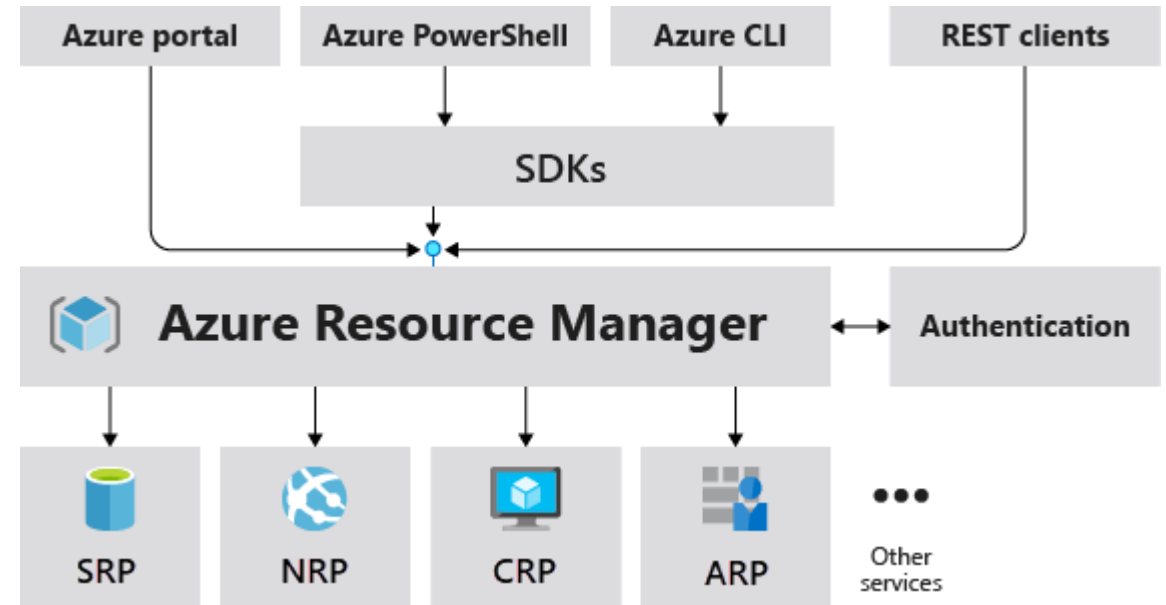
- Deployment and management service for Azure
- Enables you to create, update, and delete resources
- Provides management features, like access control, locks, and tags



[What is Azure Resource Manager? - Azure Resource Manager | Microsoft Learn](#)

Resource Providers

- Resources are created and managed by resource providers
- Each resource has a resource provider that knows how to manage and configure the resource
- Each resource provider offers a set of resources and operations for working with an Azure Service



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > Subscriptions > Visual Studio Enterprise Subscription

Visual Studio Enterprise Subscription | Resource providers

Subscription

Search

Register Unregister Refresh Feedback

Filter by name... Status : All Registration Policy : All

Provider ↑	Status
<input type="radio"/> ArizeAi.ObservabilityEval ...	✕ NotRegistered
<input type="radio"/> Astronomer.Astro ...	✕ NotRegistered
<input type="radio"/> Dell.Storage ...	✕ NotRegistered
<input type="radio"/> Dynatrace.Observability ...	✕ NotRegistered
<input type="radio"/> GitHub.Network ...	✕ NotRegistered
<input type="radio"/> Informatica.DataManagement ...	✕ NotRegistered
<input type="radio"/> LambdaTest.HyperExecute ...	✕ NotRegistered
<input type="radio"/> Microsoft.AAD ...	✕ NotRegistered
<input type="radio"/> Microsoft.ADHybridHealthService ...	✓ Registered
<input type="radio"/> Microsoft.AVS ...	✕ NotRegistered

Left sidebar navigation:

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- Resource groups
- All resources
- Recent
- App Services
- Virtual machines (classic)
- Virtual machines
- SQL databases
- Cloud services (classic)
- Subscriptions
- Microsoft Entra ID
- Monitor
- Microsoft Defender for Cloud
- Help + support
- Advisor
- Cost Management + Billing

Right sidebar navigation:

- Payment methods
- Partner information
- Settings
 - Programmatic deployment
 - Resource groups
 - Resources
 - Preview features
 - Usage + quotas
 - Policies
 - My permissions
 - Resource providers**
 - Deployments
 - Deployment stacks
 - Properties
 - Resource locks
- Help
 - Support + Troubleshooting

[Azure resource providers and types - Azure Resource Manager | Microsoft Learn](#)

<< Create a resource
 Home
 Dashboard
 All services
 ★ FAVORITES
 Resource groups
 All resources
 Recent
 App Services
 Virtual machines (classic)
 Virtual machines
 SQL databases
 Cloud services (classic)
 Subscriptions
 Microsoft Entra ID
 Monitor
 Microsoft Defender for Cloud
 Help + support
 Advisor

Dashboard > Resource groups > avs > Marketplace >

Template ...

Download Copy content Deploy Feedback

☒ Include parameters ⓘ

Template Parameters

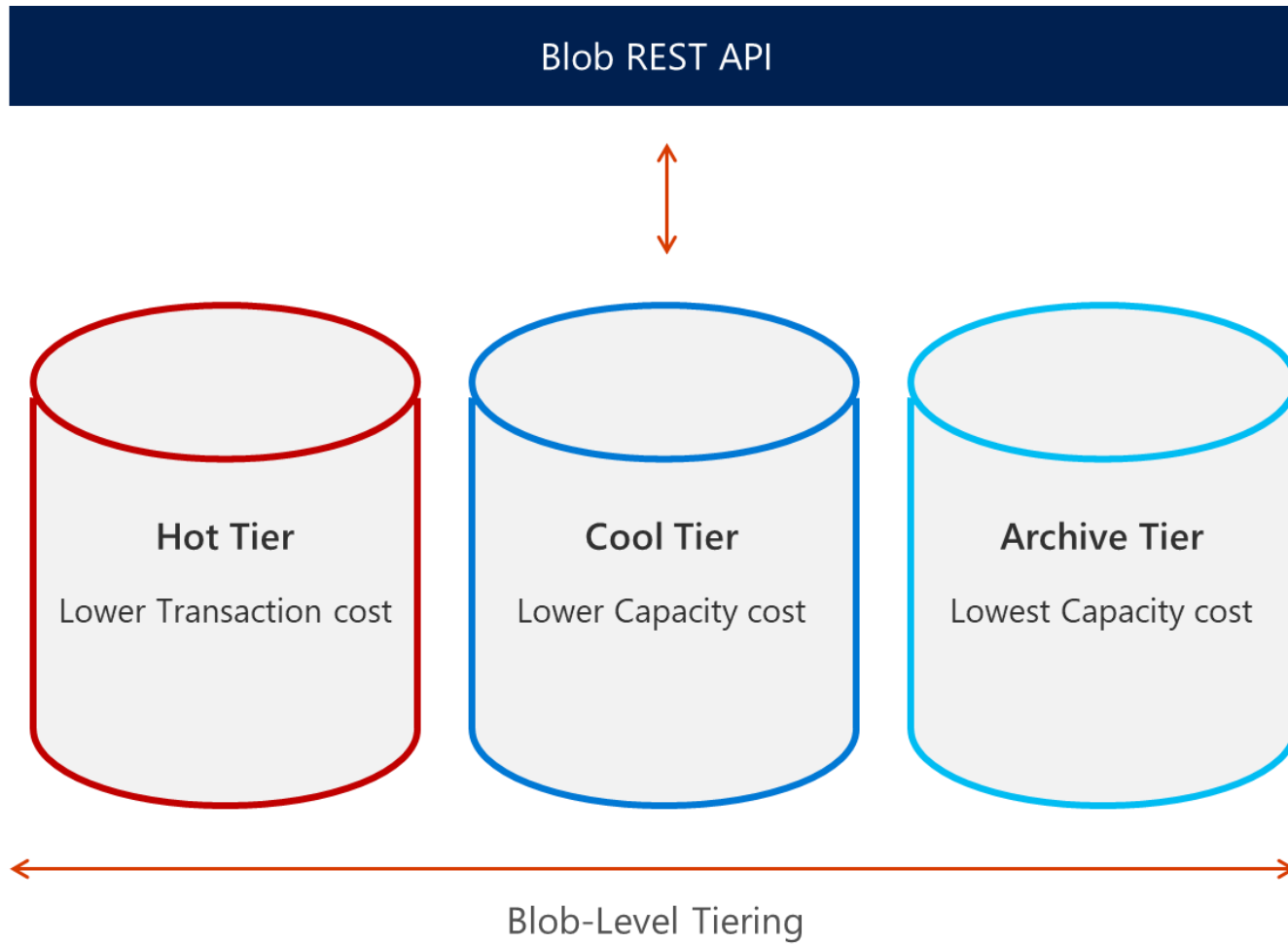
ⓘ Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define resources and configurable input parameters and deploy with script or code. [Learn more about template deployment.](#)

- > ⚙ Parameters (34)
- > 📄 Variables (4)
- ✓ 📦 Resources (4)
 - 🛡 [parameters('networkSecurityGroup')]
(Microsoft.Network/networkSecurityGroups)
 - ↔ [parameters('virtualNetworkName')]
(Microsoft.Network/virtualNetworks)
 - 💻 [parameters('virtualMachineName')]
(Microsoft.Compute/virtualMachines)
 - [concat('shutdown-computevm-', parameters('virtualMachineName'))]
(Microsoft.DevTestLab/schedules)

```

129     properties : {
130       "addressSpace": {
131         "addressPrefixes": "[parameters('addressPrefixes')]"
132       },
133       "subnets": "[parameters('subnets')]"
134     },
135     },
136     {
137       "name": "[parameters('virtualMachineName')]",
138       "type": "Microsoft.Compute/virtualMachines",
139       "apiVersion": "2024-03-01",
140       "location": "[parameters('location')]",
141       "dependsOn": [
142         "[concat('Microsoft.Network/virtualNetworks/', parameters('virtualNetworkName'))]",
143         "[concat('Microsoft.Network/networkSecurityGroups/', parameters
144           ('networkSecurityGroupName'))]"
  
```

Managing Data in Tiers



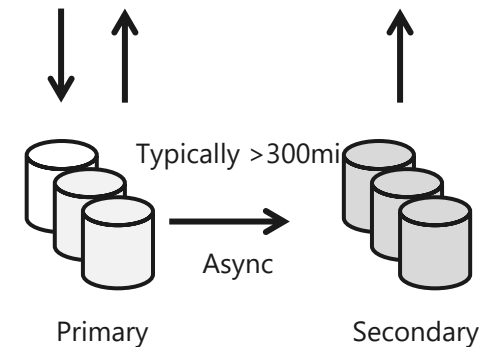
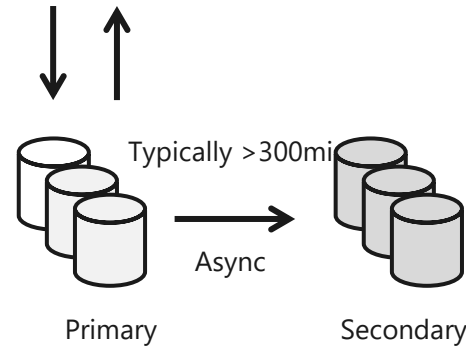
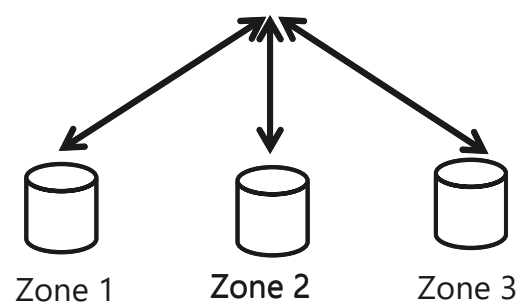
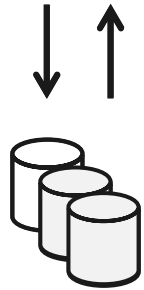
Blob-Level Tiering

Individual blobs can move between tiers
All tiers co-exist in the same storage account

Data Lifecycle Management

Automatic policy-based movement between tiers
Supports automatic deletion as well

Azure Storage Durability (Replication Options)



LRS

3 replicas, 1 region
Protect against disk, node, rack failures
Write is ack'd when all replicas are committed
Superior to dual-parity RAID
11 9s of durability

ZRS

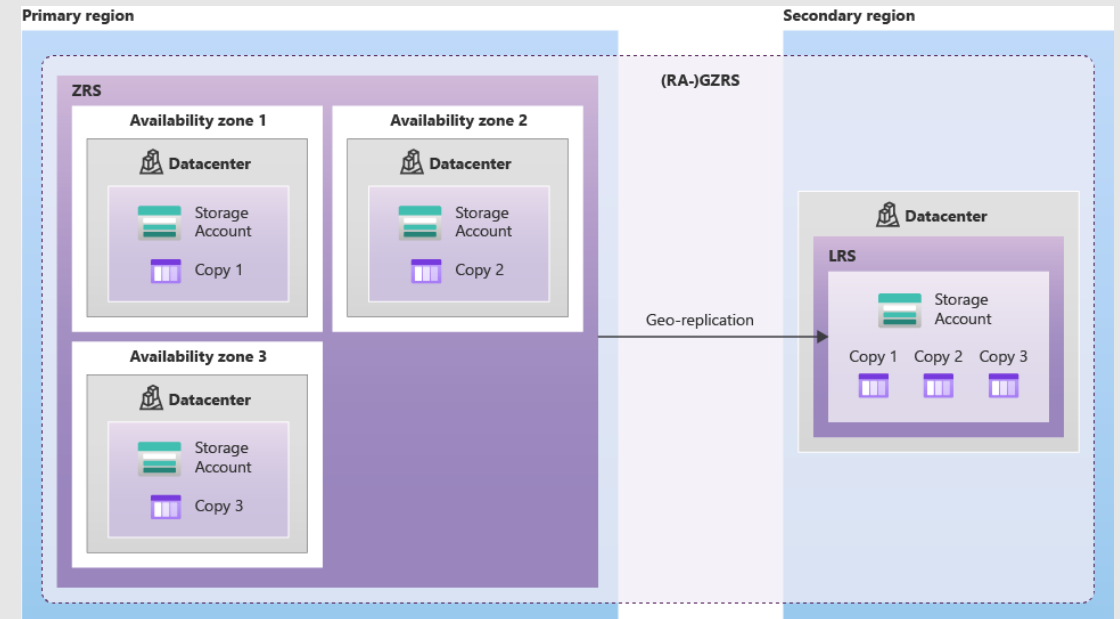
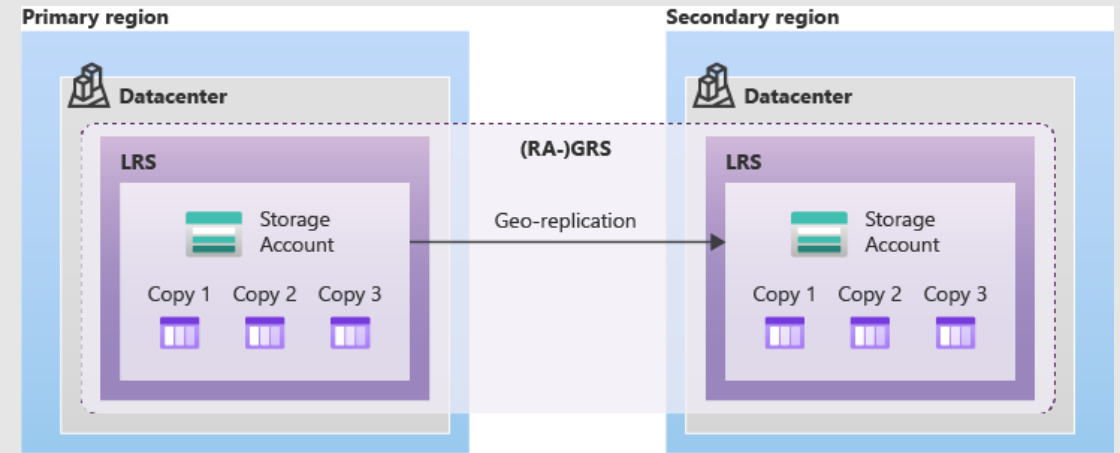
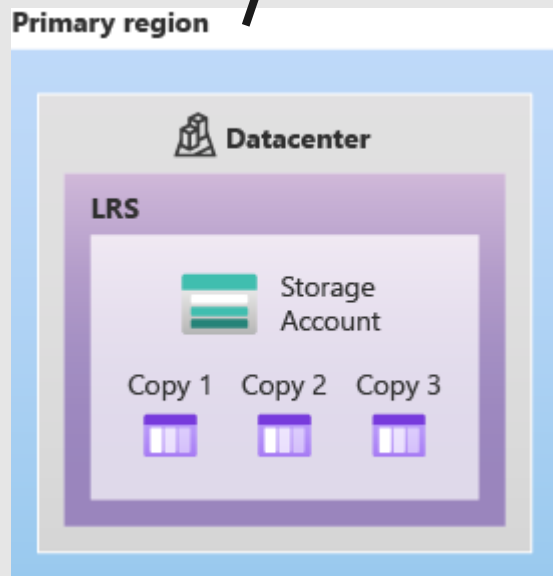
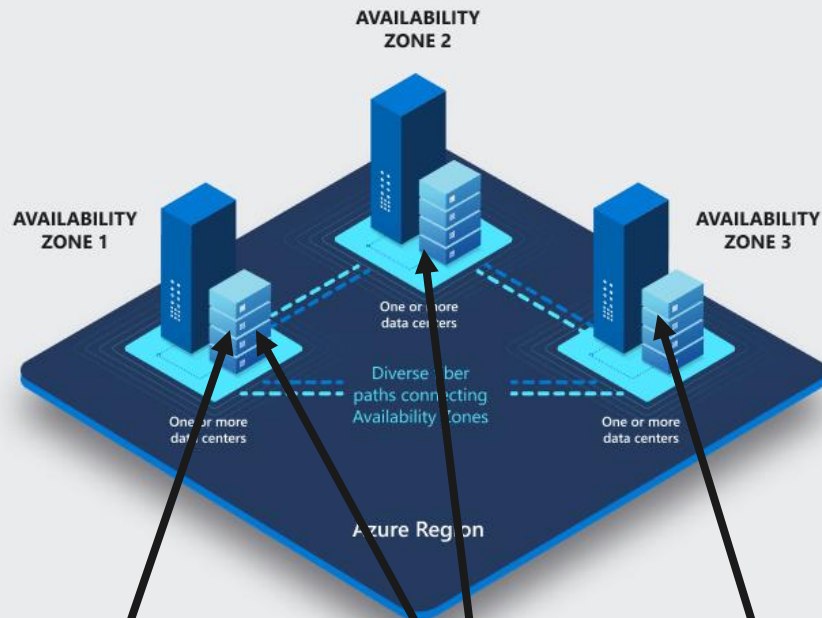
3 replicas **across 3 Zones**
Protect against disk, node, rack and **zone** failures
Synchronous writes to all 3 zones
12 9s of durability
Available in 8 regions

GRS / GRZS

6 replicas, 2 regions (3/region)
Protects against major regional disasters
Asynchronous to secondary
16 9s of durability

RA-GRS /RA_GRZS

GRS + Read access to secondary
Separate secondary endpoint
RPO delay to secondary can be queried



[Data redundancy - Azure Storage | Microsoft Learn](#)

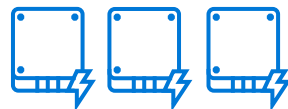
Disks Storage | Overview



Standard HDD



Standard SSD



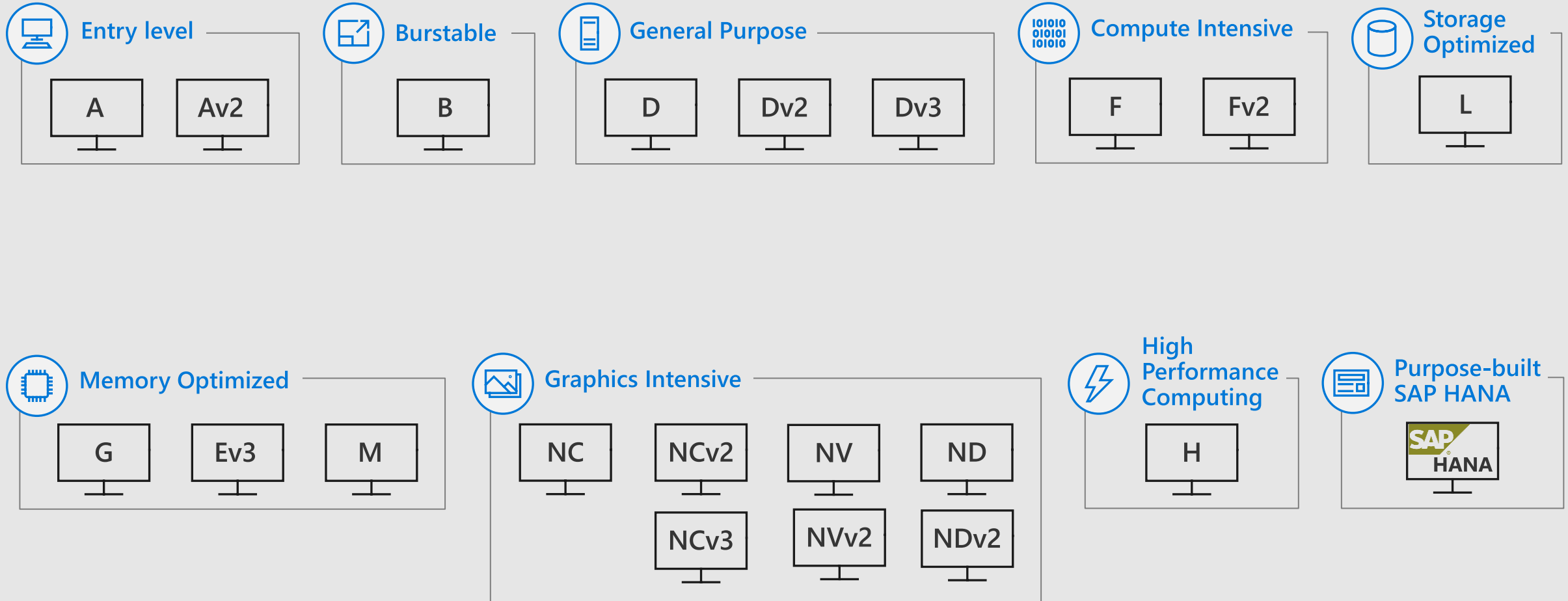
Premium SSD

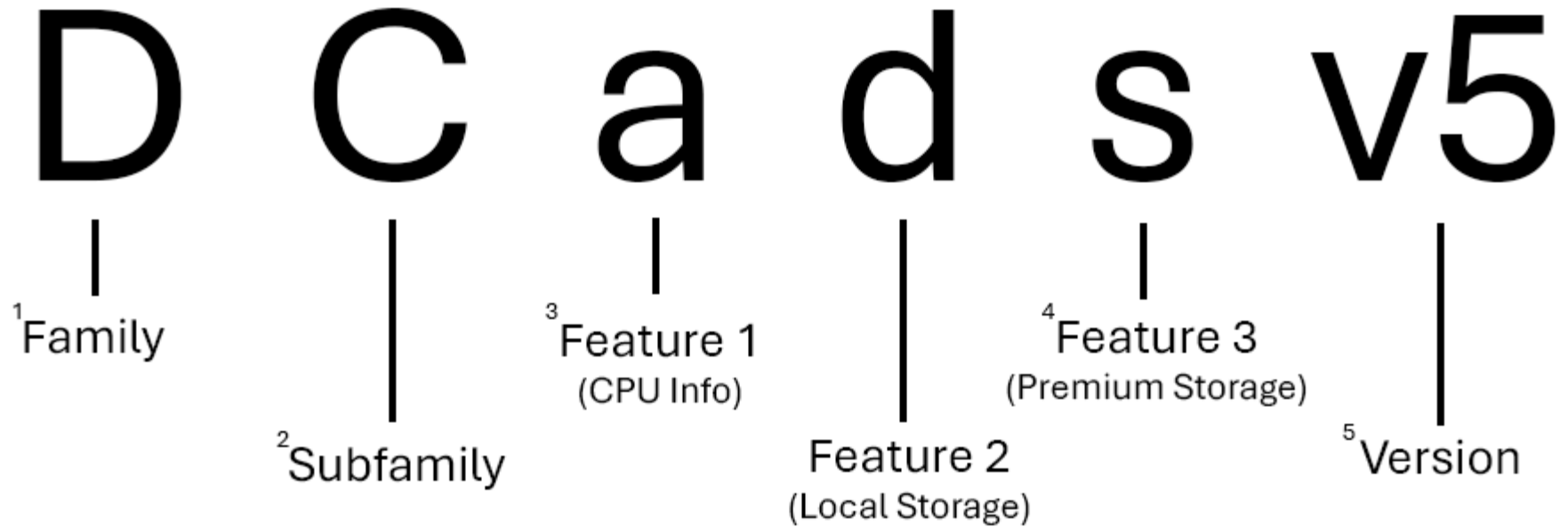


Ultra SSD

Single disk value	Low-cost storage				Consistent performance				High performance				Sub-millisecond latency			
	Max Size				Max IOPS				Max BW							
	32 TiB				Up to 2,000				Up to 500 MBps							
	8X				3-4X											

Compute options for all types of apps





¹ Most families are represented using one letter, but others such as GPU sizes (ND-series, NV-series, etc.) use two.

² Most subfamilies are represented with a single upper case letter, but others (such as Ebsv5-series) are still considered subfamilies of their parent family due to feature differences.

³ If no feature letter for a CPU is listed, the series uses Intel x86-64 CPUs. If the CPU is AMD, it's listed as a. If the CPU is ARM based (Microsoft Cobalt or Ampere Altra), it's listed as p.

⁴ There can be any number of extra features in a size name. There could be none (Dv5-series) or there could be three (DpIds_v6-series).

⁵ Version numbers only appear in the size name if there are multiple versions of the same series. If you're using the first version of a series (HB-series, B-series, etc.) it's often not included in the size name.

[Virtual machine sizes overview - Azure Virtual Machines | Microsoft Learn](#)

The screenshot displays the Azure portal interface. On the left is a navigation sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'Resource groups', 'All resources', 'Recent', 'App Services', 'Virtual machines (classic)', 'Virtual machines', 'SQL databases', 'Cloud services (classic)', 'Subscriptions', 'Microsoft Entra ID', 'Monitor', 'Microsoft Defender for Cloud', and 'Help + support'. The main area shows the 'Create a virtual machine' wizard for resource group 'azmigr_01'. It includes tabs for 'Basics', 'Disks', 'Networking', 'Management', 'Monitoring', 'Advanced', and 'Tags'. The 'Basics' tab is active, showing instructions and a 'Project details' section with dropdowns for 'Subscription' (Visual Studio Enterprise Subscription) and 'Resource group' (azmigr_01). Below this is the 'Instance details' section with fields for 'Virtual machine name', 'Region' ((Europe) West Europe), and 'Availability options' (Availability zone). On the right, the 'Copilot' sidebar is open, featuring a search bar with the query 'Which Azure service is best for shipping a highly scalable web application?'. Below the search bar is a button 'Help me choose a size for my VM'. The Copilot text states: 'To help you choose the right size for your VM, I'll need to gather more information about your specific requirements. Could you please provide details on the following:'. It lists three questions: 1. What is the primary purpose of this VM? (e.g., web server, database server, development/testing environment, data processing, etc.) 2. Do you have any specific performance or resource requirements in terms of CPU, memory, or storage? 3. Will this VM be used for production workloads or non-production (dev/test) purposes? Below the list, it says 'These details will help me make a more accurate recommendation for you.' and includes thumbs up/down icons. At the bottom of the sidebar are three suggested prompts: 'What are the best VM sizes for a web server?', 'How much CPU and memory do I need for a database server?', and 'What VM size is suitable for a development environment?'.

Home > Resource groups > azmigr_01 > Marketplace >

Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Visual Studio Enterprise Subscription

Resource group * ⓘ azmigr_01
[Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ (Europe) West Europe

Availability options ⓘ Availability zone

Copilot

Which Azure service is best for shipping a highly scalable web application?

Help me choose a size for my VM

Copilot AI-generated content may be incorrect

To help you choose the right size for your VM, I'll need to gather more information about your specific requirements. Could you please provide details on the following:

1. What is the primary purpose of this VM? (e.g., web server, database server, development/testing environment, data processing, etc.)
2. Do you have any specific performance or resource requirements in terms of CPU, memory, or storage?
3. Will this VM be used for production workloads or non-production (dev/test) purposes?

These details will help me make a more accurate recommendation for you.

What are the best VM sizes for a web server?

How much CPU and memory do I need for a database server?

What VM size is suitable for a development environment?

Security & Management

-  Security Center
-  Portal
-  Azure Active Directory
-  Azure AD B2C
-  Multi-Factor Authentication
-  Automation
-  Scheduler
-  Key Vault
-  Store/Marketplace
-  VM Image Gallery & VM Depot

Platform Services






Media & CDN

-  Media Services
-  Media Analytics
-  Content Delivery Network








Integration

-  API Management
-  BizTalk Services
-  Logic Apps
-  Service Bus







Compute Services

-  Container Service
-  VM Scale Sets
-  Batch
-  RemoteApp
-  Dev/Test Lab








Application Platform

-  Web Apps
-  Mobile Apps
-  API Apps
-  Cloud Services
-  Service Fabric
-  Notification Hubs
-  Functions

Developer Services

-  Visual Studio
-  Mobile Engagement
-  VS Team Services
-  Xamarin
-  Application Insights
-  HockeyApp











Data

-  SQL Database
-  SQL Data Warehouse
-  DocumentDB
-  SQL Server Stretch Database
-  Redis Cache
-  Storage Tables
-  Azure Search









Intelligence

-  Cognitive Services
-  Bot Framework
-  Cortana

Analytics & IoT

-  HDInsight
-  Machine Learning
-  Stream Analytics
-  Data Catalog
-  Data Lake Analytics Service
-  Data Lake Store
-  IoT Hub
-  Event Hubs
-  Data Factory
-  Power BI Embedded

Hybrid Cloud

-  Azure AD Health Monitoring
-  AD Privileged Identity Management
-  Domain Services
-  Backup
-  Operational Analytics
-  Import/Export
-  Azure Site Recovery
-  StorSimple

Infrastructure Services

Compute

-  Virtual Machines
-  Containers

Storage

-  Blob
-  Queues
-  Files
-  Disks

Networking

-  Virtual Network
-  Load Balancer
-  DNS
-  Express Route
-  Traffic Manager
-  VPN Gateway
-  App Gateway

Datacenter Infrastructure



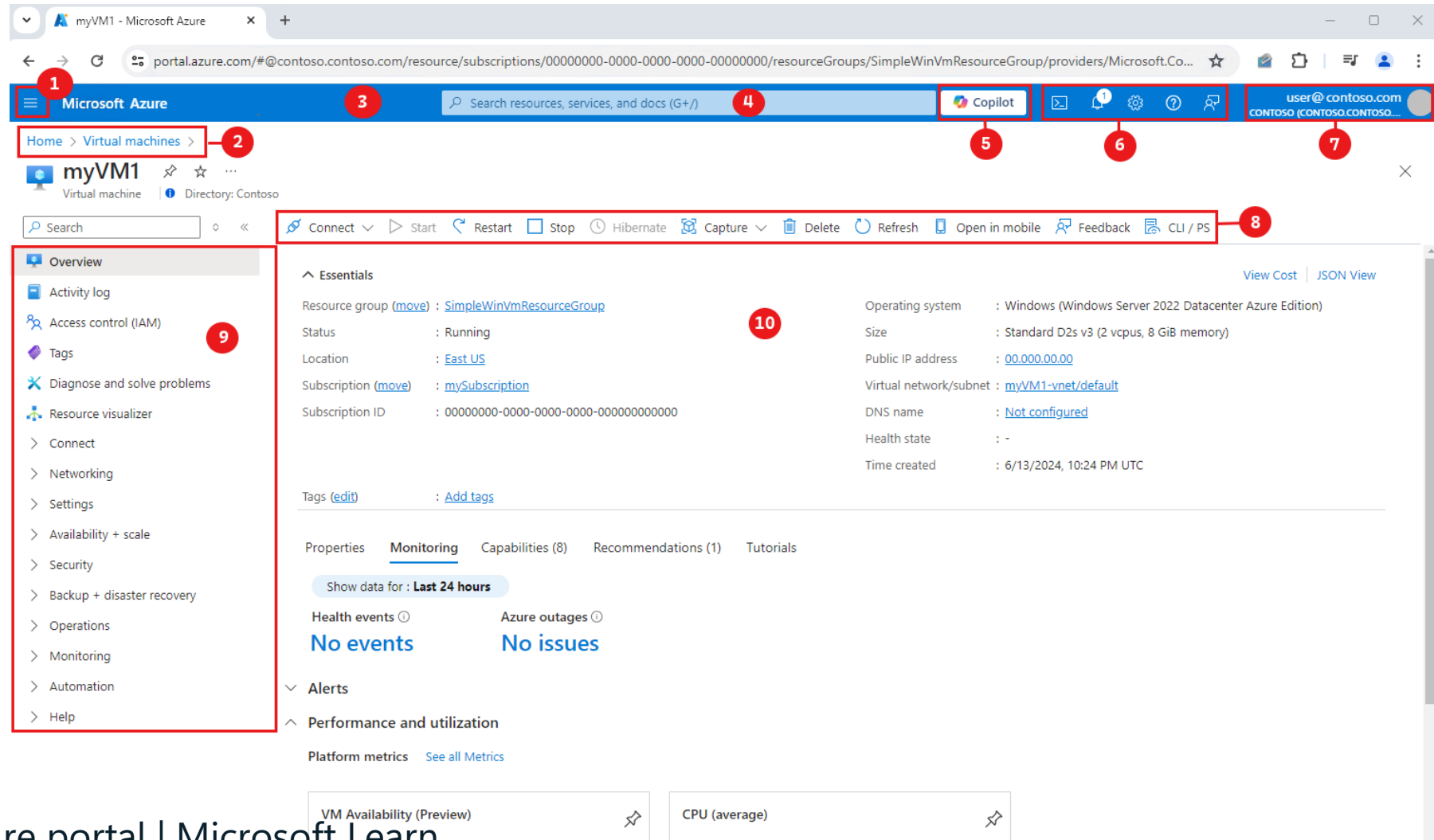


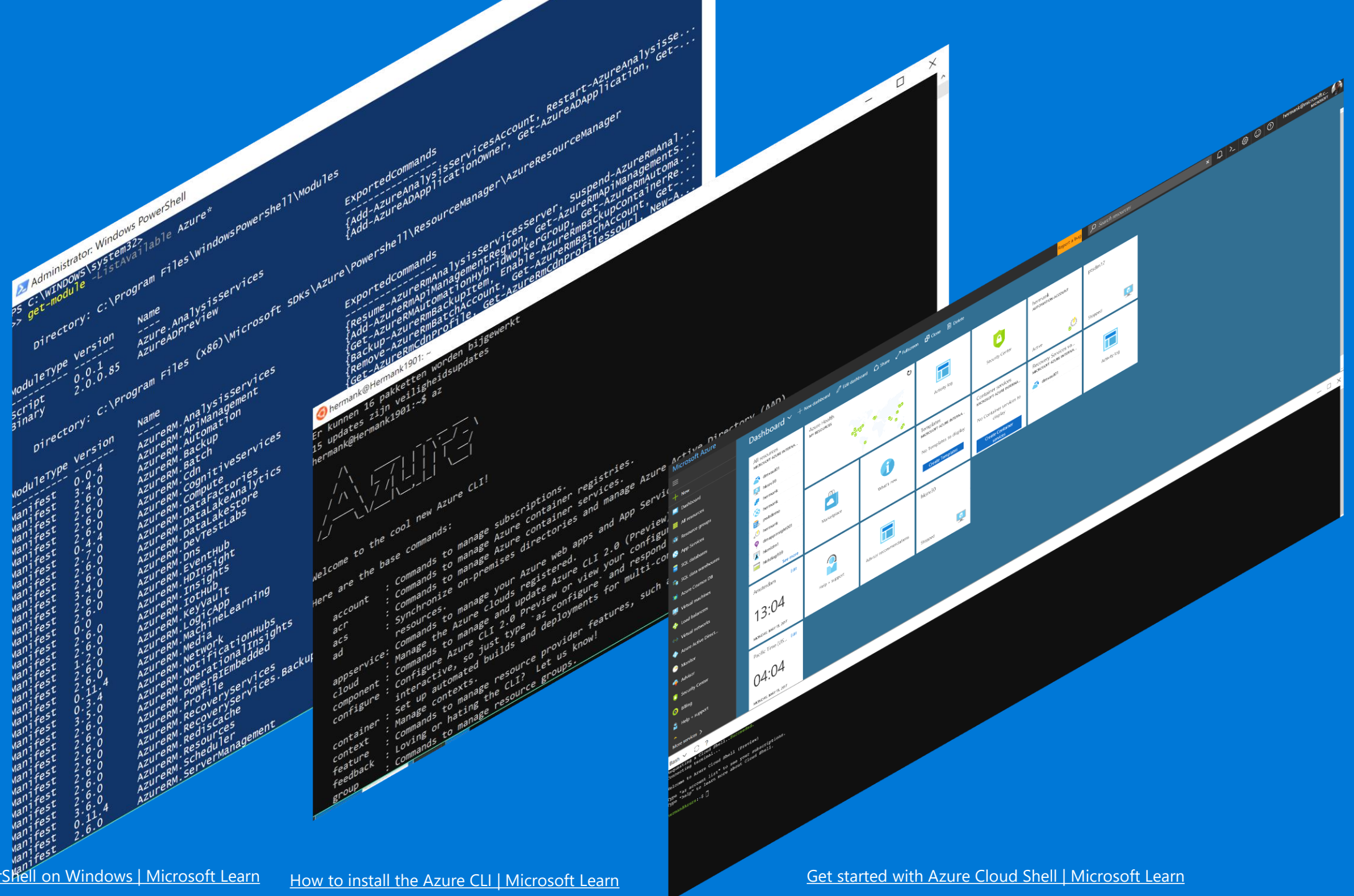
The Azure Portal

The Azure Portal

Key user interface elements

- 1 – Portal Menu
- 2 – Breadcrumb
- 3 – Page header
- 4 – Global search
- 5 – Copilot
- 6 – Global controls
- 7 – Your account
- 8 – Command bar
- 9 – Service menu
- 10 – Working pane





Maintaining an Azure environment

Tagging is mandatory for better accountability

Tag your resources

Tags should be enforced by configuration policy

Use Azure Policy to set and track ARM tagging policies

Tags should include 3 types of information

Billing information: cost center, billing ID, etc.

Ownership information: whom should be contacted when needed

Purpose information: environment, application service, etc.

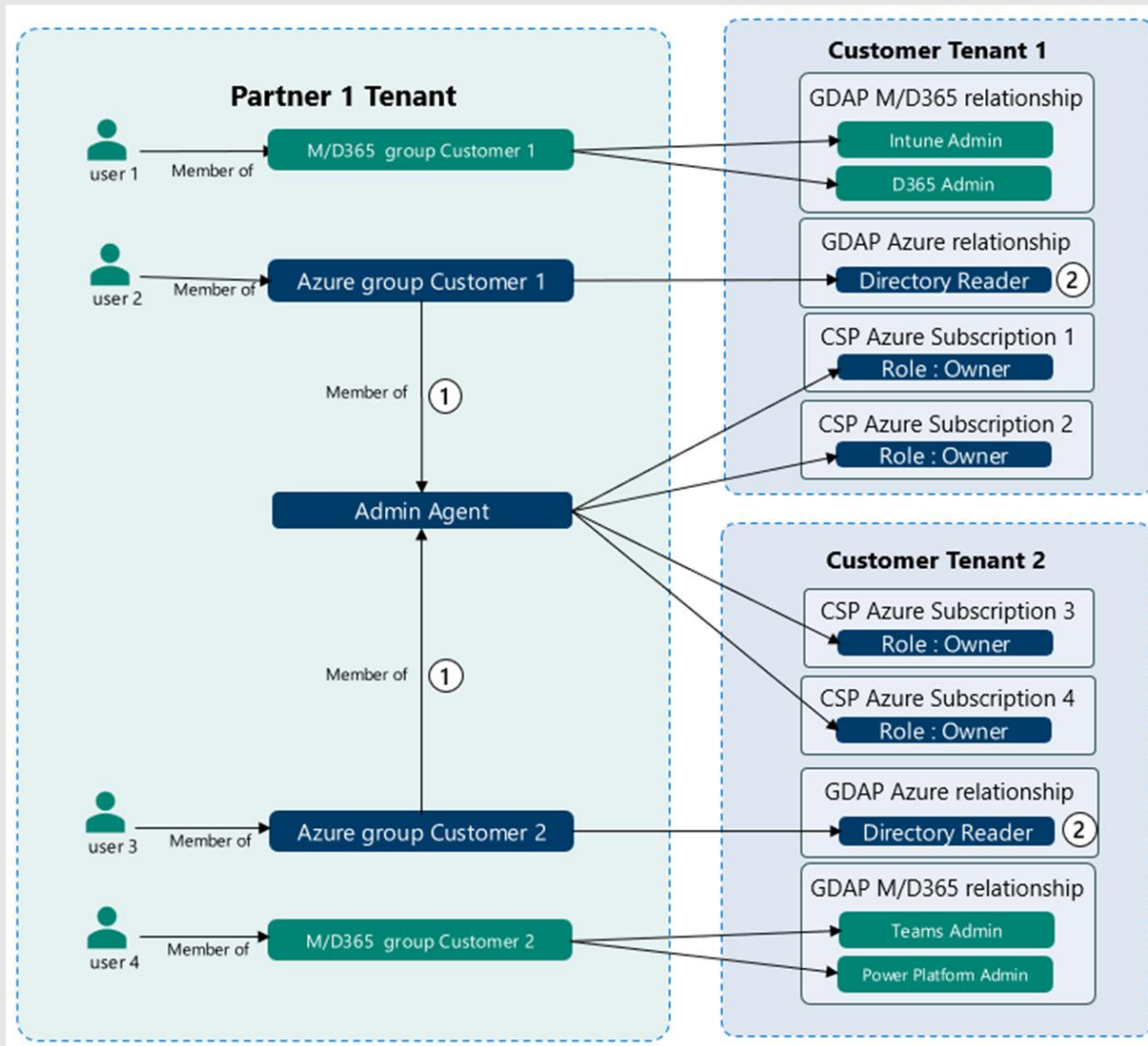
Cost Management can help

Discovers ARM Resource Group tags and automatically associate to underlying resources

Has rules for standardizing, rewriting, adding meta-tag values

[Using tags to organize your Azure resources](#)

GDAP

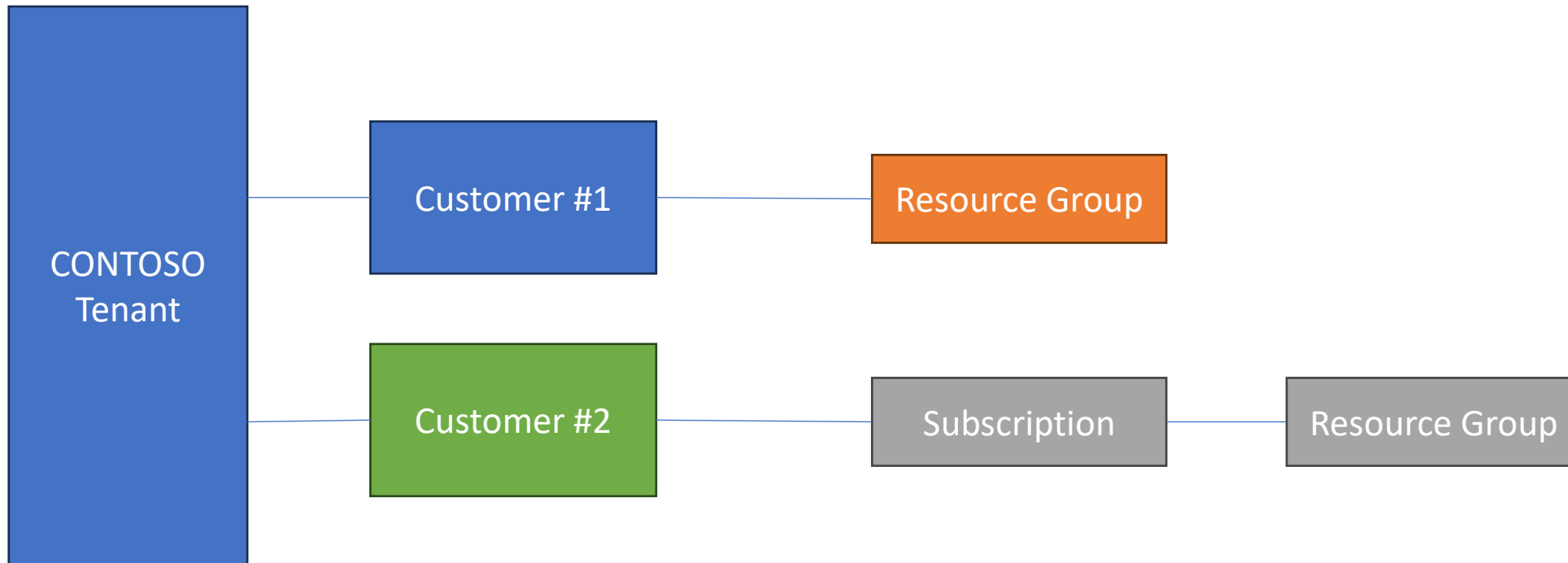


Granular Delegated Admin Privileges (GDAP) is a security feature in Microsoft's Partner Center that allows partners to have least-privileged access to their customers' workloads. This feature is designed to follow the Zero Trust cybersecurity protocol, ensuring that partners only have the necessary permissions to perform their tasks

[GDAP role guidance - Partner Center | Microsoft Learn](#)

[GDAP frequently asked questions - Partner Center | Microsoft Learn](#)

Azure Lighthouse works



Azure delegated resource management creates a logical projection of resources from one tenant onto another tenant. This lets authorized service provider users sign in to their own tenant, with authorization to work in delegated customer subscriptions and resource groups with the roles they were granted during the onboarding process. Users in the service provider's tenant can then perform management operations on behalf of their customers, without having to sign in to each individual customer tenant.

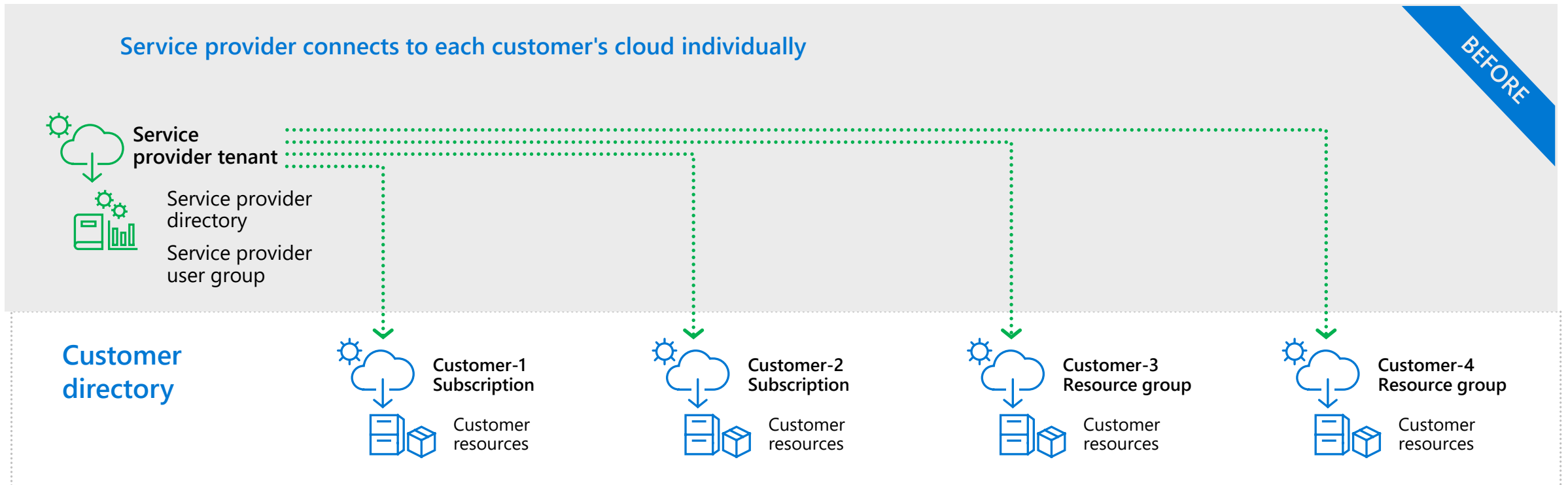
[What is Azure Lighthouse? - Azure Lighthouse | Microsoft Learn](#)

[Onboard a customer to Azure Lighthouse - Azure Lighthouse | Microsoft Learn](#)

Azure Lighthouse secret sauce: Design customer capabilities in partner environments with Azure delegated resource management

Client features, designed in the service provider tenant to be managed by authorized service provider users

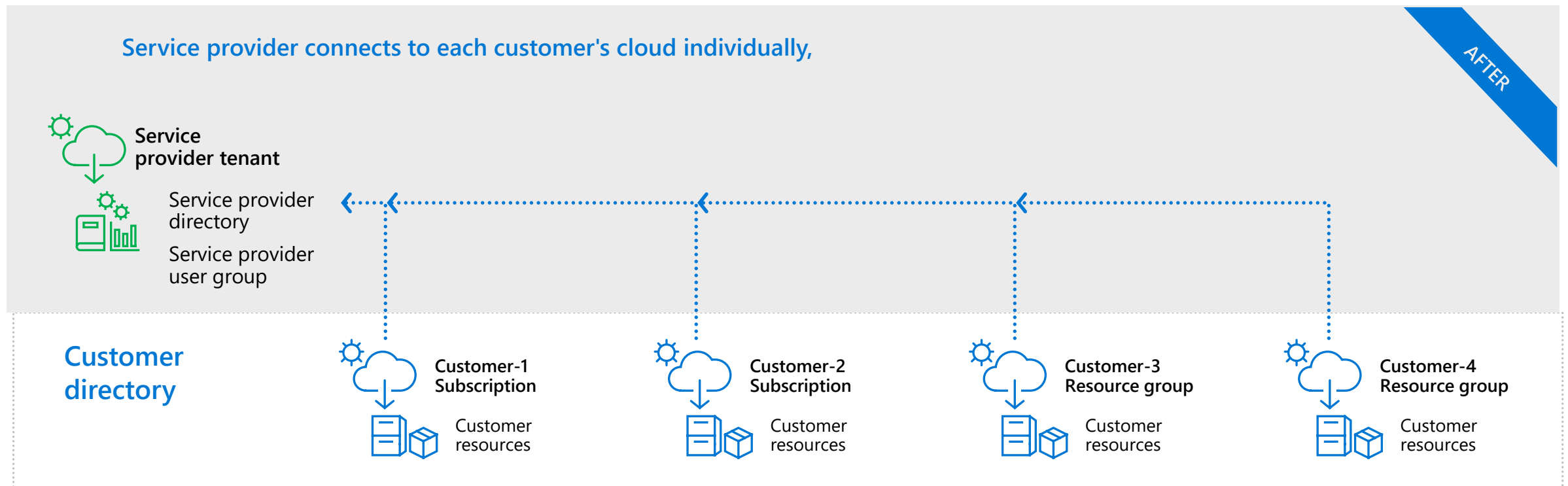
The service provider can perform operations at the Create, Read, Update, Delete (CRUD) scope)



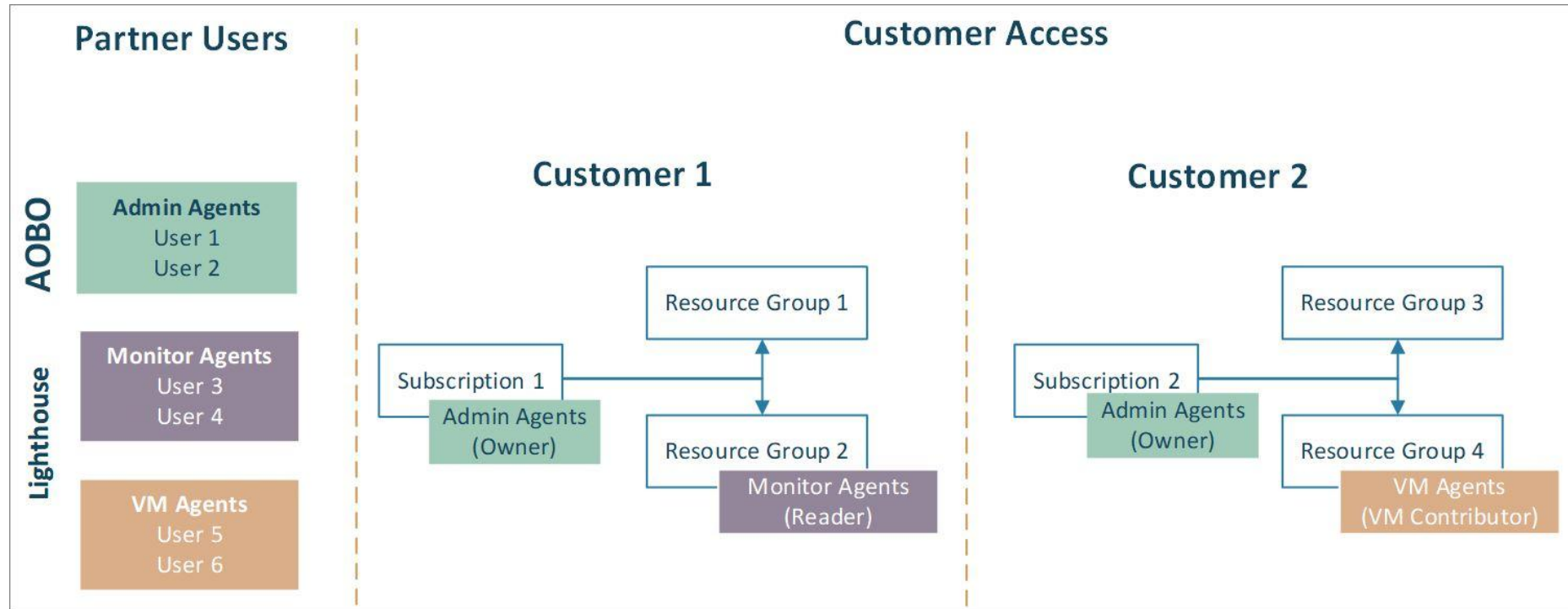
Azure Lighthouse secret sauce: Design customer capabilities in partner environments with Azure delegated resource management

Client features, designed in the service provider tenant to be managed by authorized service provider users

The service provider can perform operations at the Create, Read, Update, Delete (CRUD) scope)

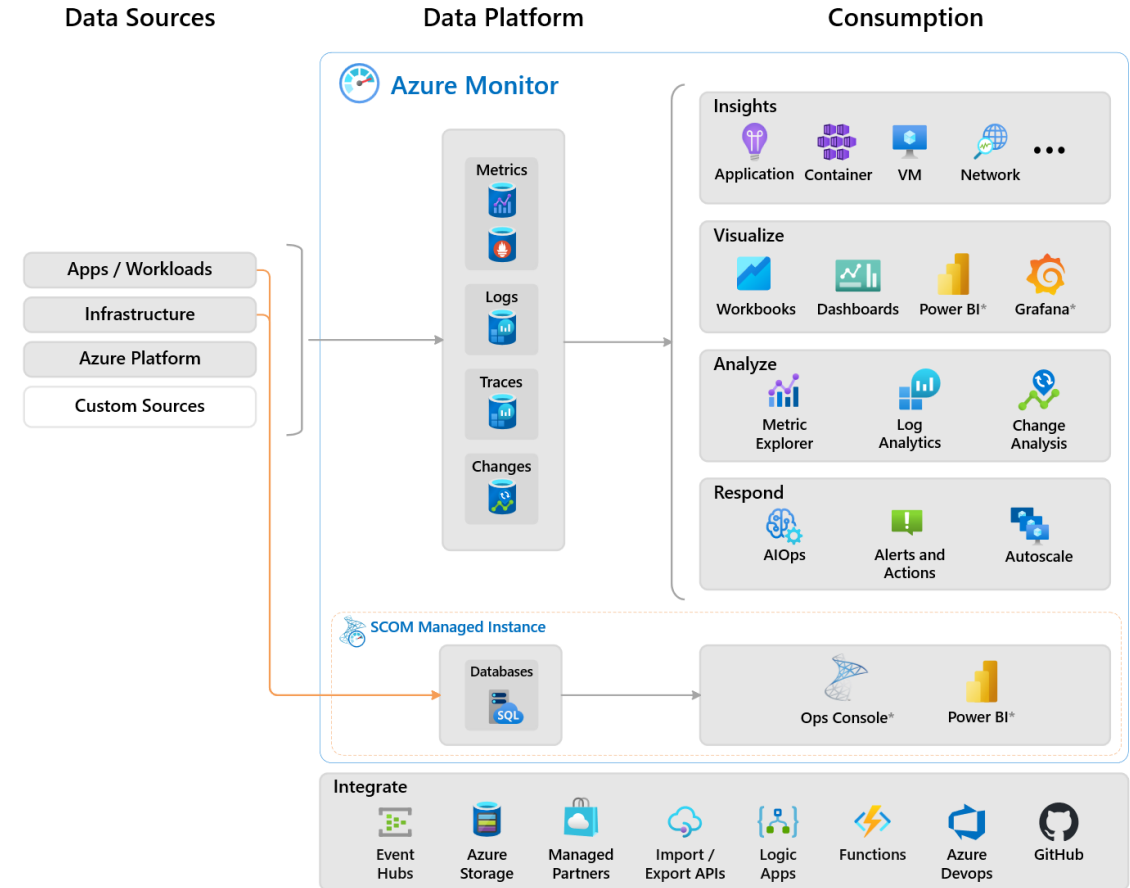


Azure lighthouse and CSP



Monitor

- ➔ Detect & diagnose issues across **apps and dependencies** with application insights
- ➔ Correlate issues at **infra level** with insights for VMs, containers, storage, network, etc.
- ➔ Operationalize at scale with smart **alerts** and automated **actions**
- ➔ Drill down with **log analytics** for troubleshooting & deeper diagnostics
- ➔ Create **visualizations** with Azure dashboards, workbooks & Grafana



Microsoft Azure

Search resources, services, and docs (G+ /)

Copilot

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

All resources

Recent

App Services

Virtual machines (classic)

Virtual machines

SQL databases

Cloud services (classic)

Subscriptions

Microsoft Entra ID

Monitor

Microsoft Defender for Cloud

Help + support

Advisor

Cost Management + Billing

Dashboard >

Monitor | Overview

Microsoft

Search

Overview

Activity log

Alerts

Metrics

Logs

Change Analysis

Service health

Workbooks

Dashboards with Grafana (preview)

Insights

Applications

Virtual Machines

Storage accounts

Containers

Networks

Azure Cosmos DB

Key Vaults

The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Az to this date.

Overview

Tutorials

Insights

Use curated monitoring views for specific Azure resources. [View all insights](#)

Application insights

Monitor your app's availability, performance, errors, and usage.

View More

Container Insights

Gain visibility into the performance and health of your controllers, nodes, and containers.

View More

VM Insights

Monitor the health, performance, and dependencies of your VMs and VM scale sets.

View More

Network Insights

View the health and metrics for all deployed network resources.

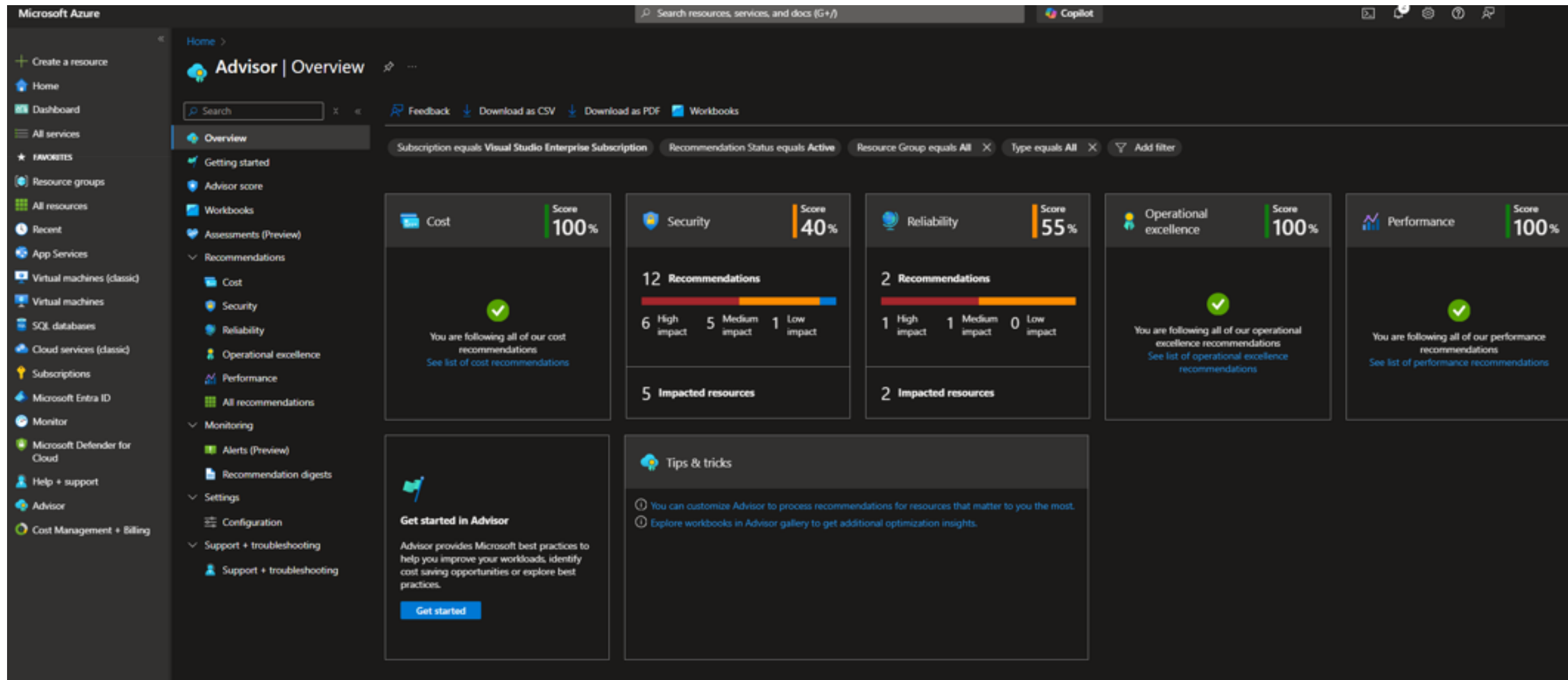
View More

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. [Learn more about monitoring](#)

Metrics

Alerts



Introduction to Azure Advisor - Azure Advisor | Microsoft Learn

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

All resources

Recent

App Services

Virtual machines (classic)

Virtual machines

SQL databases

Cloud services (classic)

Subscriptions

Microsoft Entra ID

Monitor

Microsoft Defender for Cloud

Help + support

Advisor

Cost Management + Billing

Dashboard >

Microsoft Defender for Cloud | Overview

Showing subscription 'Visual Studio Enterprise Subscription'

Search

Subscriptions

What's new

General

Overview

Setup

Recommendations

Attack path analysis

Security alerts

Inventory

Cloud Security Explorer

Workbooks

Community

Diagnose and solve problems

Cloud Security

Security posture

Regulatory compliance

Workload protections

Data and AI security

Firewall Manager

1

Azure subscriptions

5

Assessed resources

--

Attack paths

--

Security alerts

Security posture

0

Critical recommendations

0

Attack paths

0/0

Overdue recommendations

Environment risk and secure score

All recommendations by risk (12)

Critical 0

High 0

Medium 1

Low 11

Not evaluated 0

Total secure score

40%

Azure 40%

AWS -

GCP -

Explore your security posture >

Microsoft Defender for Cloud Overview - Microsoft Defender for Cloud | Microsoft Learn

Azure Arc

Management services



Portal



Copilot



Graph



Identity



Defender



Monitor



Updates



Policy



Support



Billing

Cloud region

Distributed location



Enabled by
Azure Arc

Popular



Windows
and Linux



Azure Virtual
Desktop



Azure IoT
Operations

App services



App Service



Functions



Logic Apps

Data services



Arc-enabled
SQL Server



Managed
instance



PostgreSQL

AI services

NEW



Video
Indexer

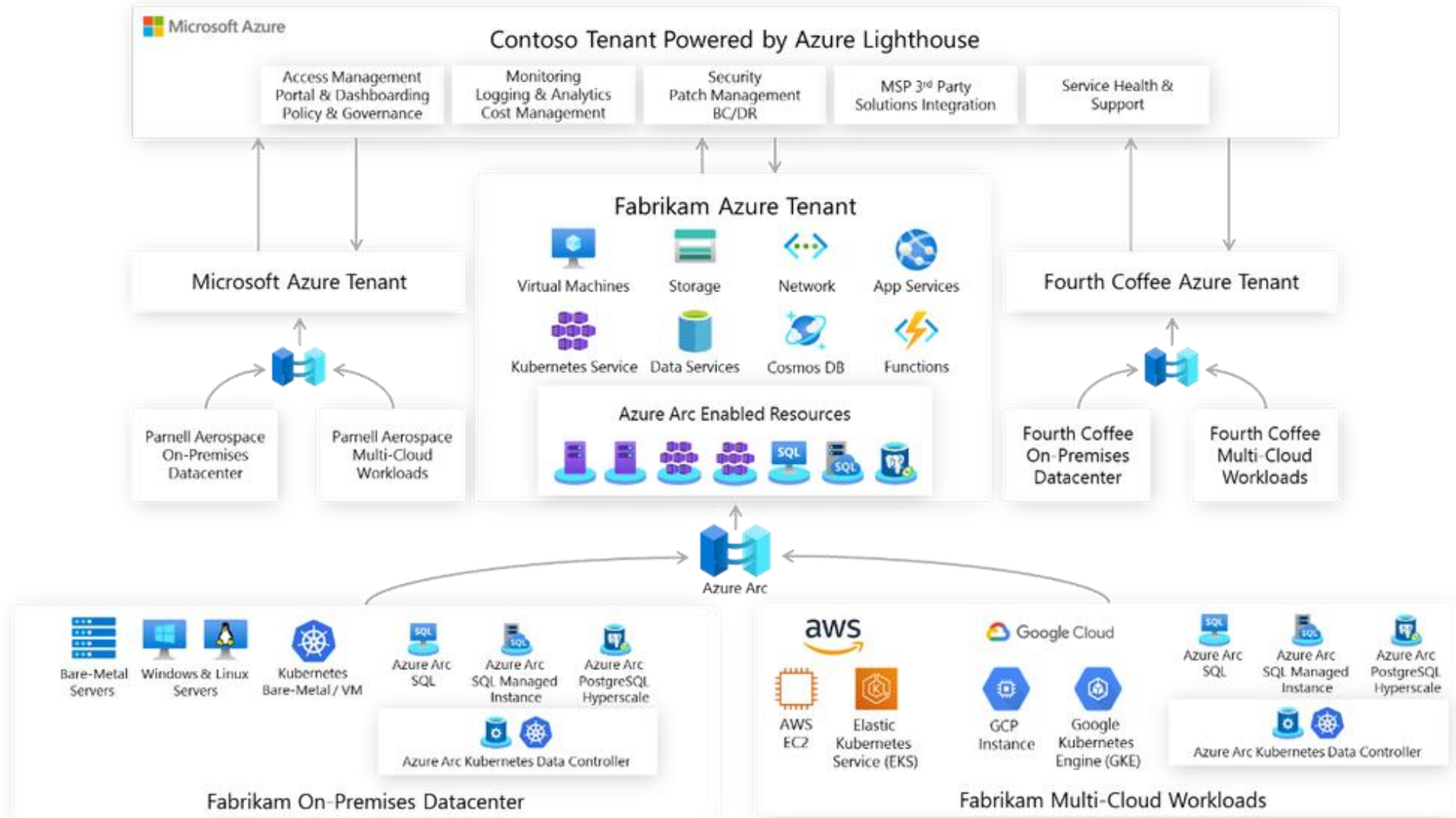


Local AI search
(preview)



Machine
Learning

Extend Azure management across your environments



Azure documentation

Learn how to build and manage powerful applications using Microsoft Azure cloud services. Get documentation, example code, tutorials, and more.



GET STARTED
Get started for Azure developers



TRAINING
[Build skills with Microsoft Learn for Azure](#)



ARCHITECTURE
Design your app using the Azure Architecture Center



OVERVIEW
Achieve organizational goals with the Cloud Adoption Framework

Browse Azure products

Popular

Popular

AI + Machine Learning

Analytics

Compute

Containers

Databases

Developer Tools

DevOps

Hybrid + multicloud

Identity

Integration

Internet of Things

Management and Governance

Media



App Service

Quickly create powerful cloud apps for web and mobile



Azure AI Foundry

Build market-ready applications for your organization with AI



Azure Arc

Bring Azure services and management to any infrastructure



Azure Cosmos DB

Fast NoSQL database with open APIs for any scale



Azure Functions

Process events with serverless code



Azure Kubernetes Service (AKS)

Simplify the deployment, management, and operations of Kubernetes



Azure Operator Insights

Analyze network data from multiple sources



Azure Quantum (Preview)

Experience quantum impact today on Azure

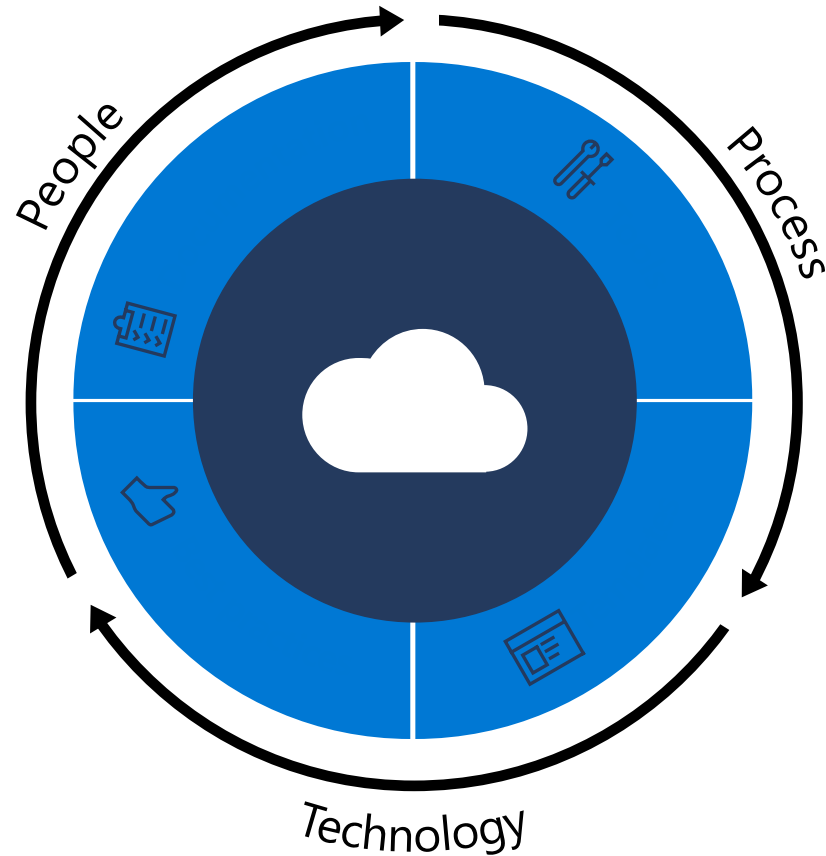
What next

- Landing zones
- Compliance (zero trust)
 - [Trust-center](#)
- CSP

Thank you

Azure landing zone

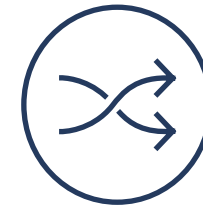
Microsoft Cloud Adoption Framework for Azure



Control
& Stability



Speed
& Results



Achieve balance

Align business, people and technology strategy.

Achieve business goals with actionable, efficient, and comprehensive guidance.

Deliver fast results with control and stability.

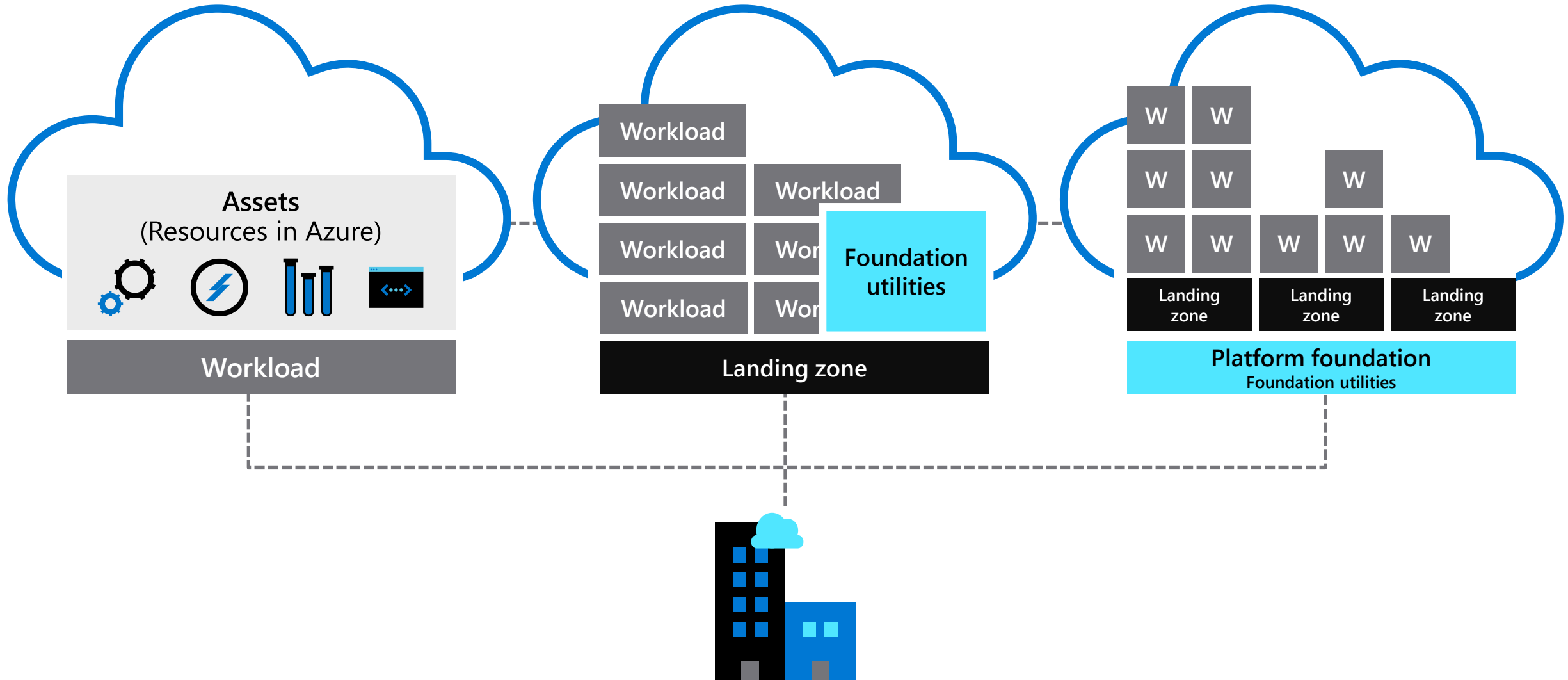
Microsoft Cloud Adoption Framework for Azure



Cloud operating model



Foundations in the cloud

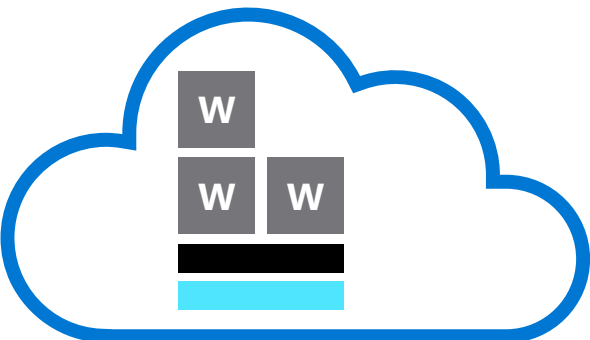


Align the foundation—

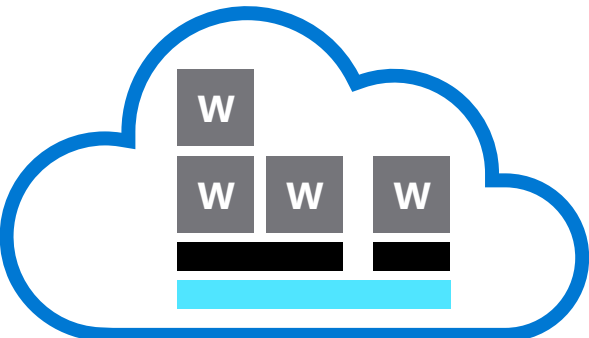
to *your* chosen cloud operating model



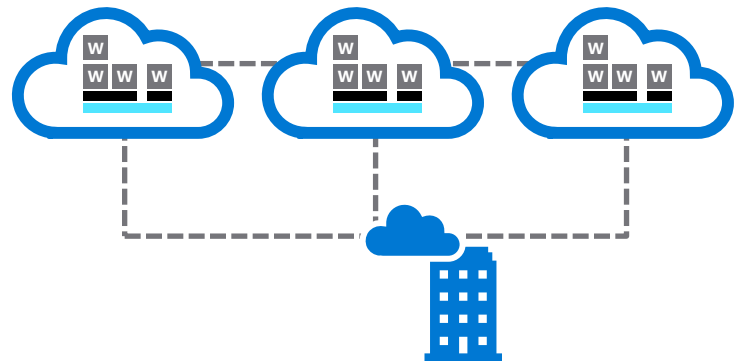
Decentralized operations



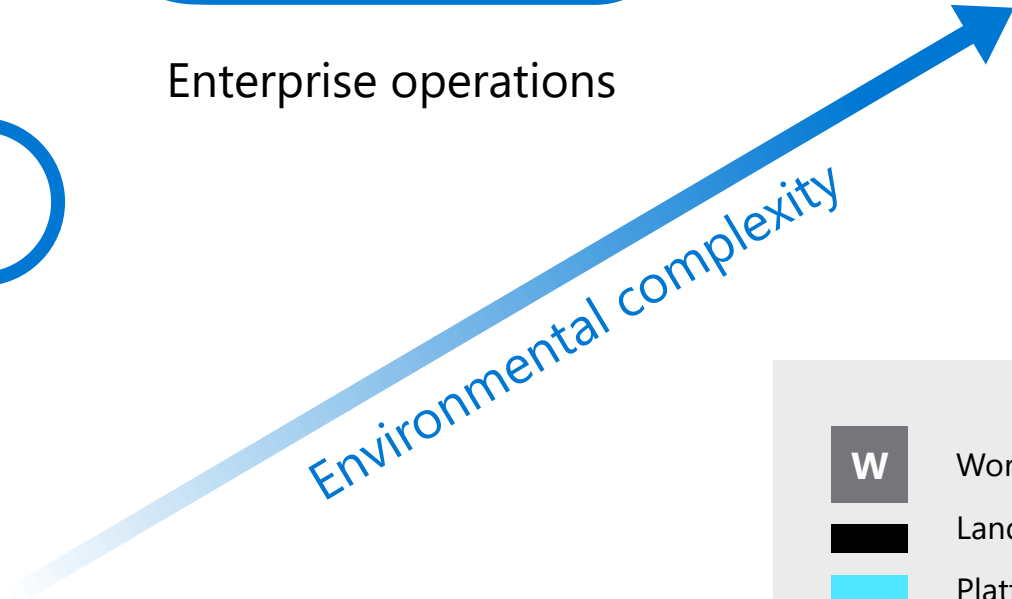
Central operations



Enterprise operations



Distributed operations



W

Workload

Landing zones

Platform foundation

Decentralized operations

Azure landing zones



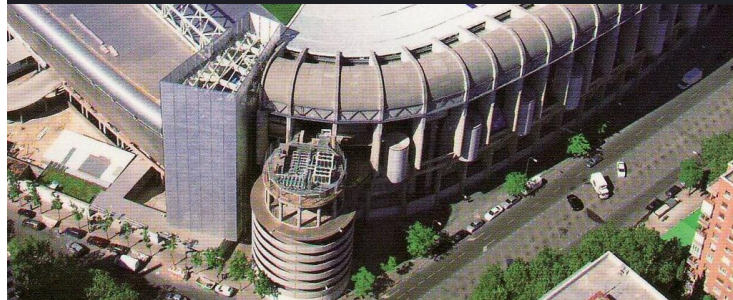
What are you building?



House



Stadium



Bridge



What are **landing zones** for?

- ❑ **Starting a journey based on best practices** with a start-to-finish plan is a key factor for success
- ❑ **Creating well-designed foundations** for a cloud environment will enable the safe adoption of new technologies, at pace
- ❑ **Using consistent, repeatable environment designs** helps scaling out in a manageable way
- ❑ **Baking in repeatable best practices** into environment deployments
- ❑ **Factoring your team's technical skills** into environment planning

Azure landing zones

Do



Azure billing &
Azure Active Directory tenant



Identity & access
management

ENVIRONMENT



Resource organization



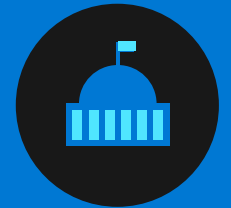
Network topology
& connectivity

COMPLIANCE

Security



Governance



Management



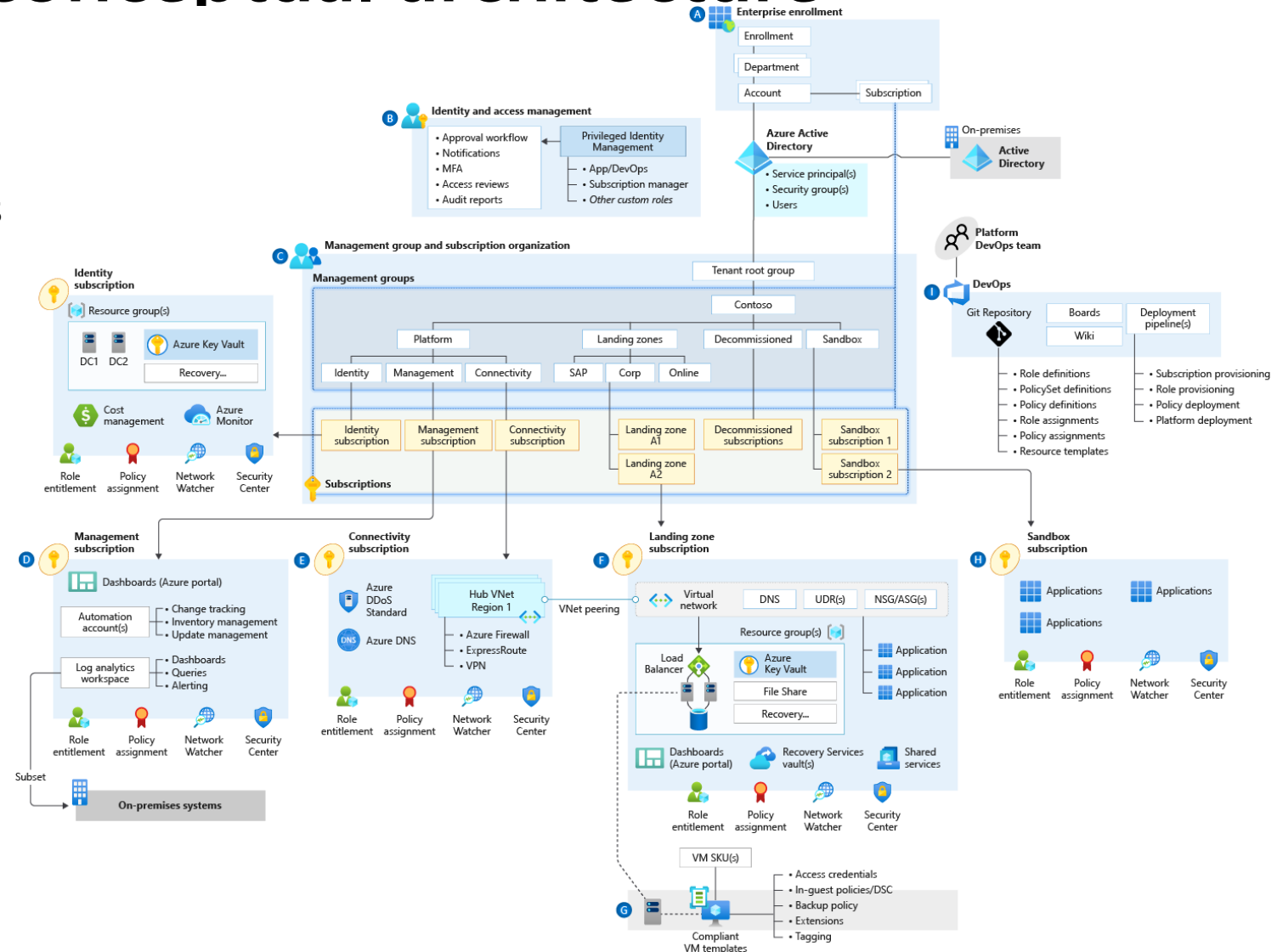
Platform automation
& DevOps



Azure landing zone conceptual architecture

What does it represent?

- ✓ **Target end-state** for most organizations
- ✓ **Scaled-out and mature** environment
- ✓ **Customer and partner practices** for environment design **across Microsoft**
- ✓ **Strong foundation for management, governance, and security** processes



Azure landing zone deployment options

Azure landing zone accelerator (portal)

- Fastest path to the target architecture
- Implements environmental design practices
- Implements opinionated compliance design best practices

Alternative approaches for customized Azure landing zones



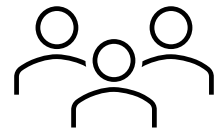
Azure Resource Manager



Azure Bicep



HashiCorp Terraform



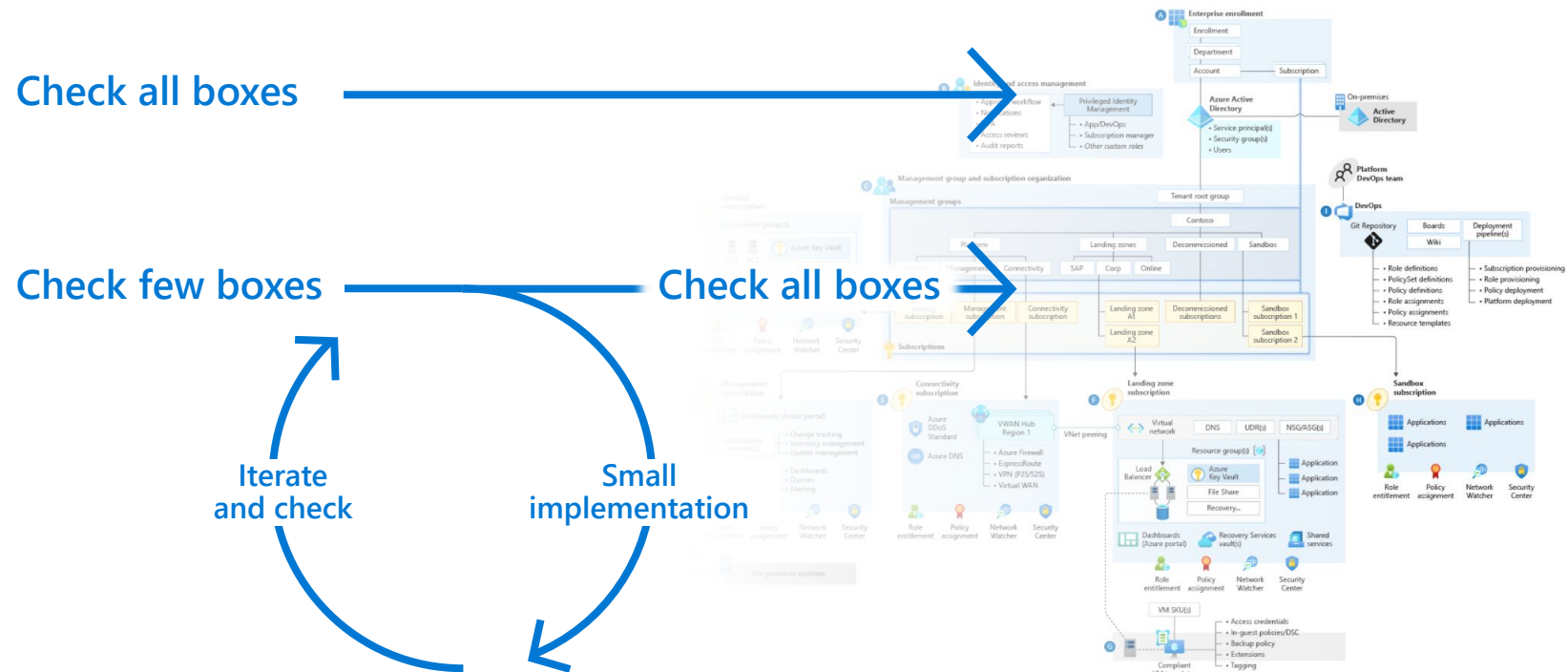
Partner

Common implementation approach



- ☐ Azure billing and AD tenant
- ☐ Identity and access management
- ☐ Network topology and connectivity
- ☐ Resource organization
- ☐ Governance
- ☐ Management
- ☐ Security
- ☐ Platform automation and DevOps

Target end-state:
Azure landing zones conceptual architecture



Azure landing zone Design Principles (1 of 6)

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



Subscription Democratisation



Policy Driven Governance



Single Control and Management Plane



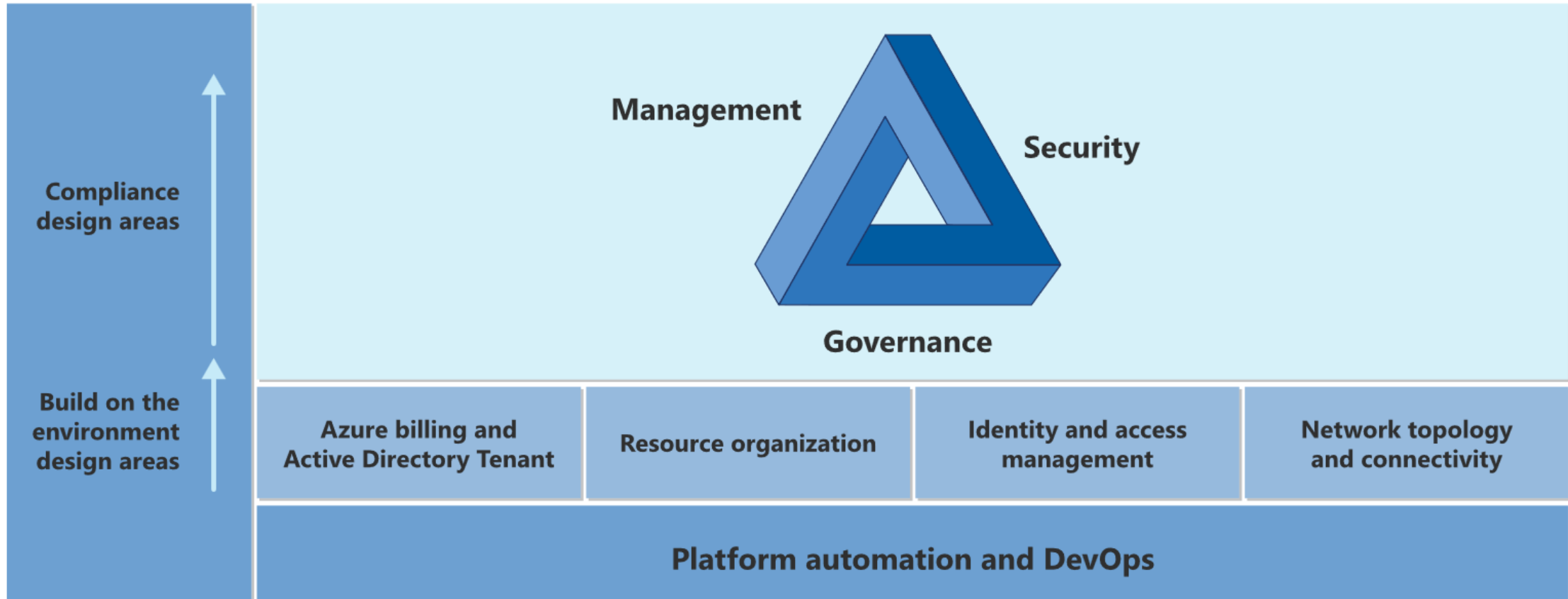
Application Centric and Archetype-Neutral



Azure Native Design and Platform Roadmap Alignment

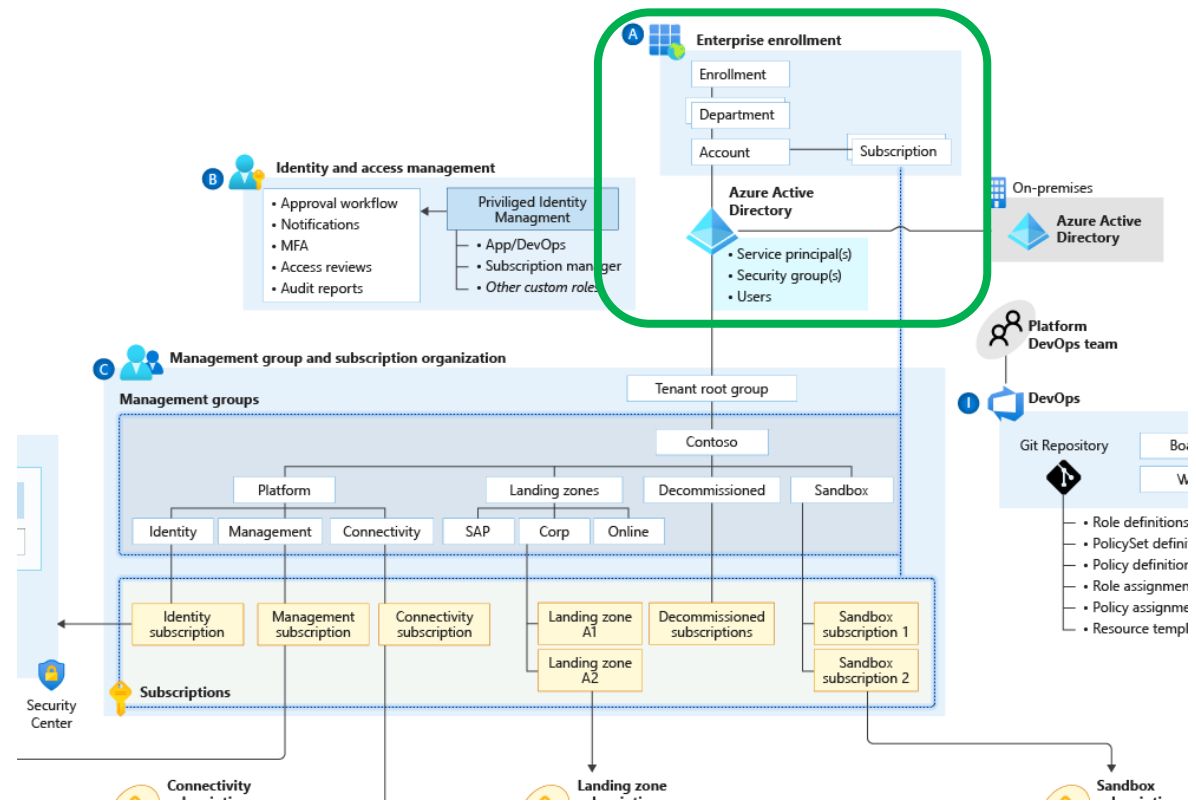
Azure landing zones

Design areas





Azure billing & Active Directory tenant



Enterprise enrolment roles links users with their **functional role** and consists of

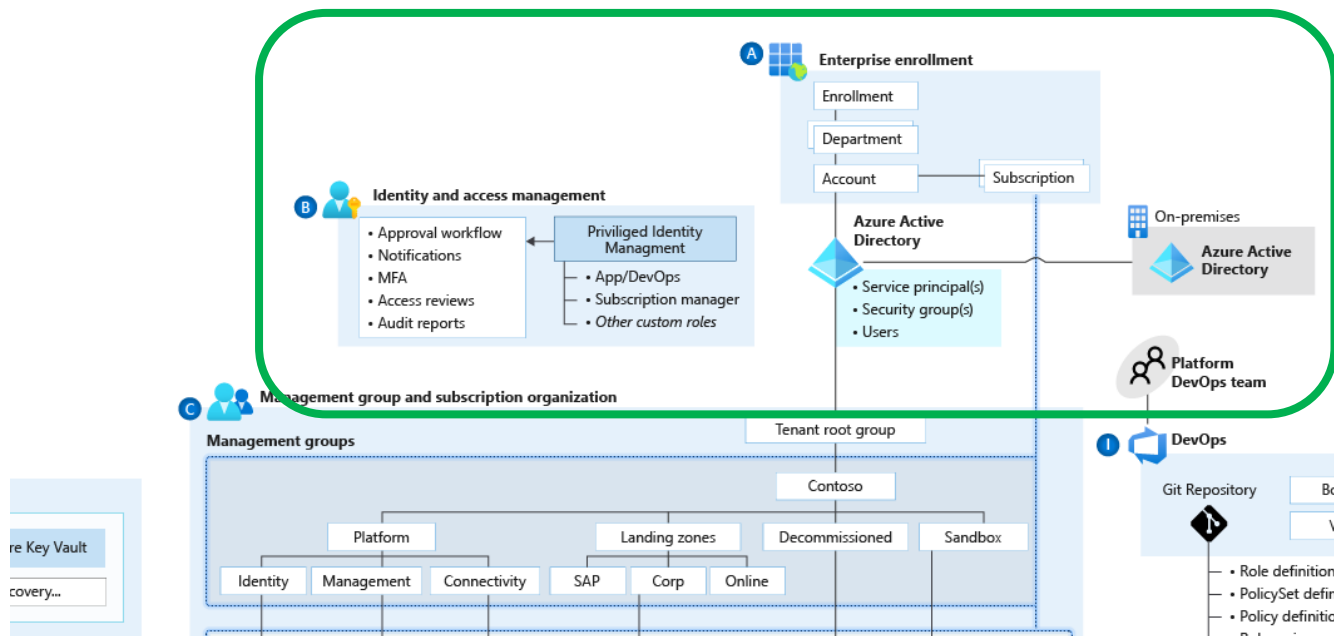
- ☐ Enterprise Administrator
- ☐ Department Administrator
- ☐ Account Owner
- ☐ Service Administrator
- ☐ Notification Contact

Define Azure AD
Tenants



Identity & Access Management

Planning for Authentication Inside the Landing Zone



A critical design decision enterprise organization must make when adopting Azure is whether to:

☐ **extend** an existing on-premises identity domain into Azure

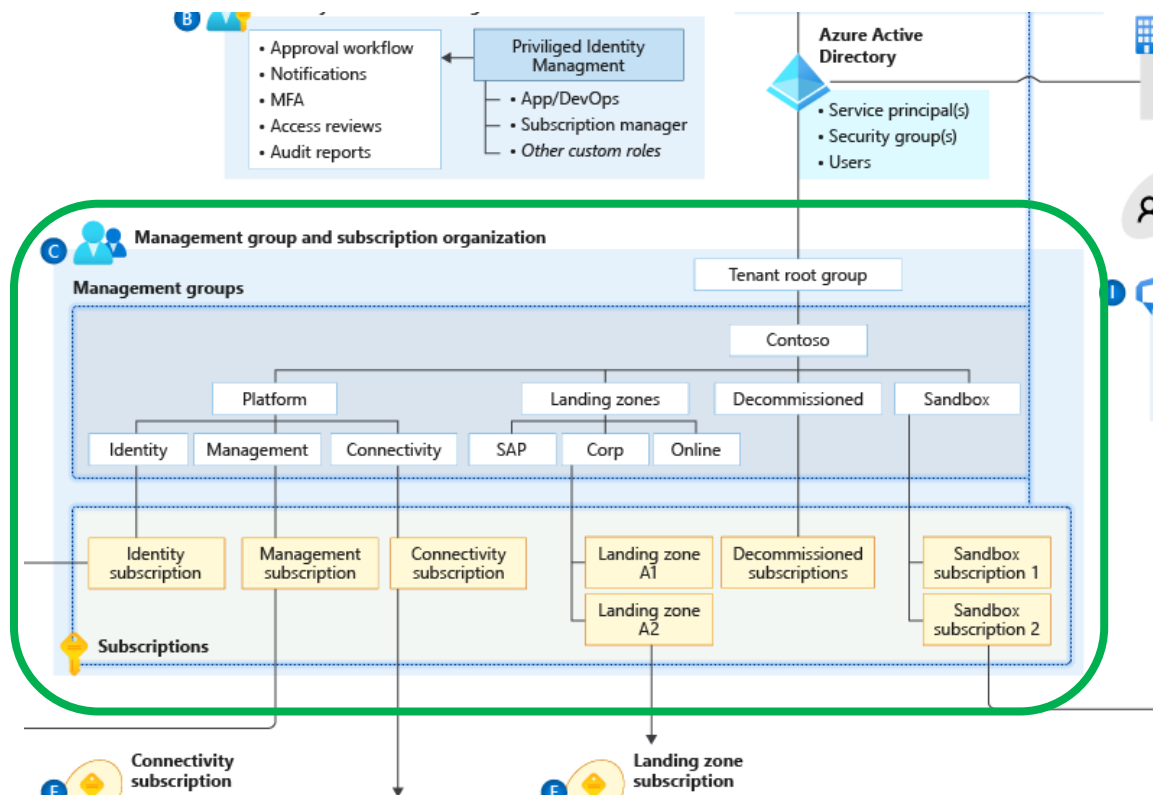
or

☐ **create** a brand new one



Resource organization

Define Hierarchy,
Quota & Capacity,
and Manage Cost



Subscription Organization and Governance

- ❑ Use Management Group structure, within an AAD tenant, to support org mapping
- ❑ Must be appropriately considered when planning Azure adoption at-scale

Configure Subscription Quota and Capacity

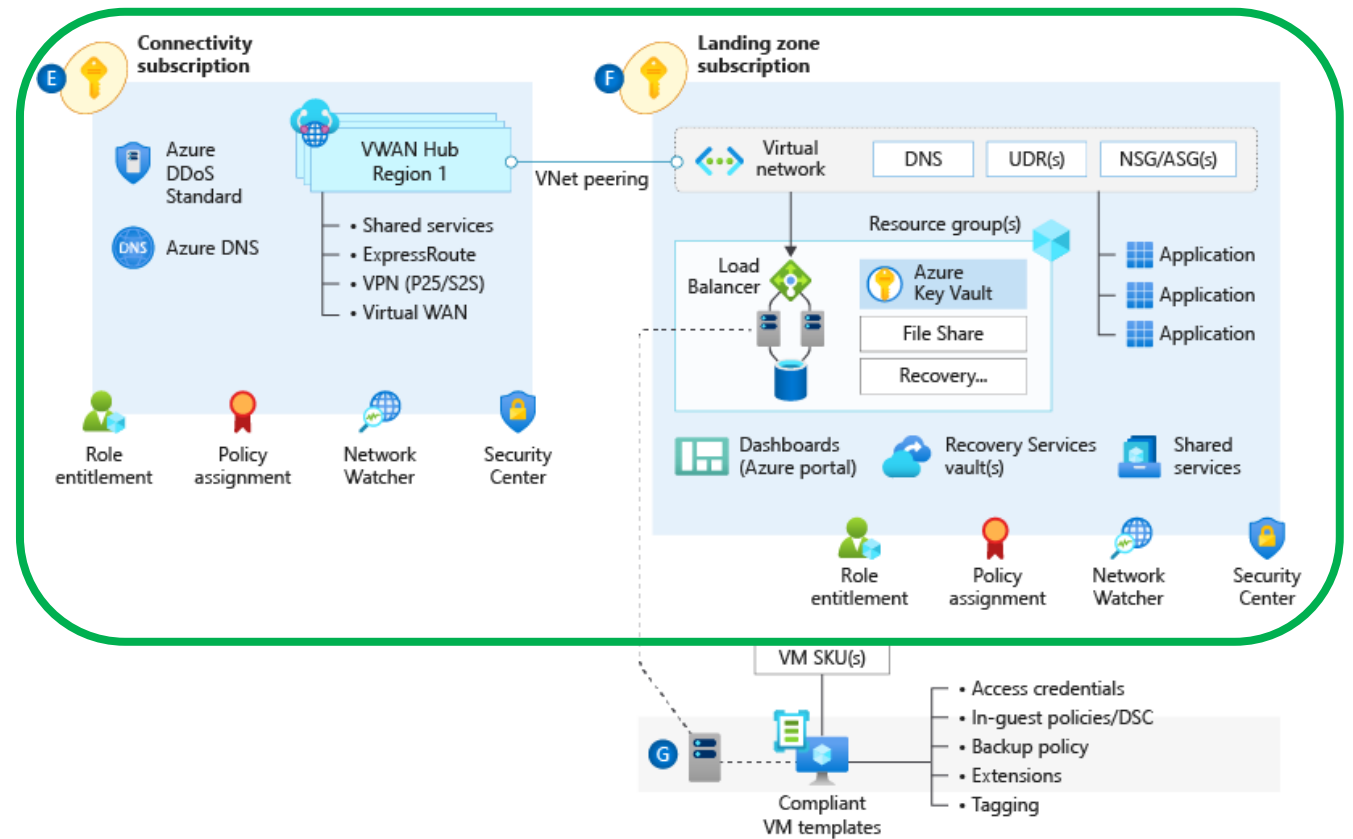
- ❑ Platform limits and quotas within the Azure platform for services
- ❑ Availability of required SKUs in chosen Azure regions
- ❑ Subscription quotas are not capacity guarantees and are per region

Establish Cost Management

- ❑ Potential need for chargeback models where shared PaaS services are concerned, such as ASE which may need to be shared to achieve higher density
- ❑ Shutdown schedule for non-prod workloads to optimise costs



Network Topology & Connectivity



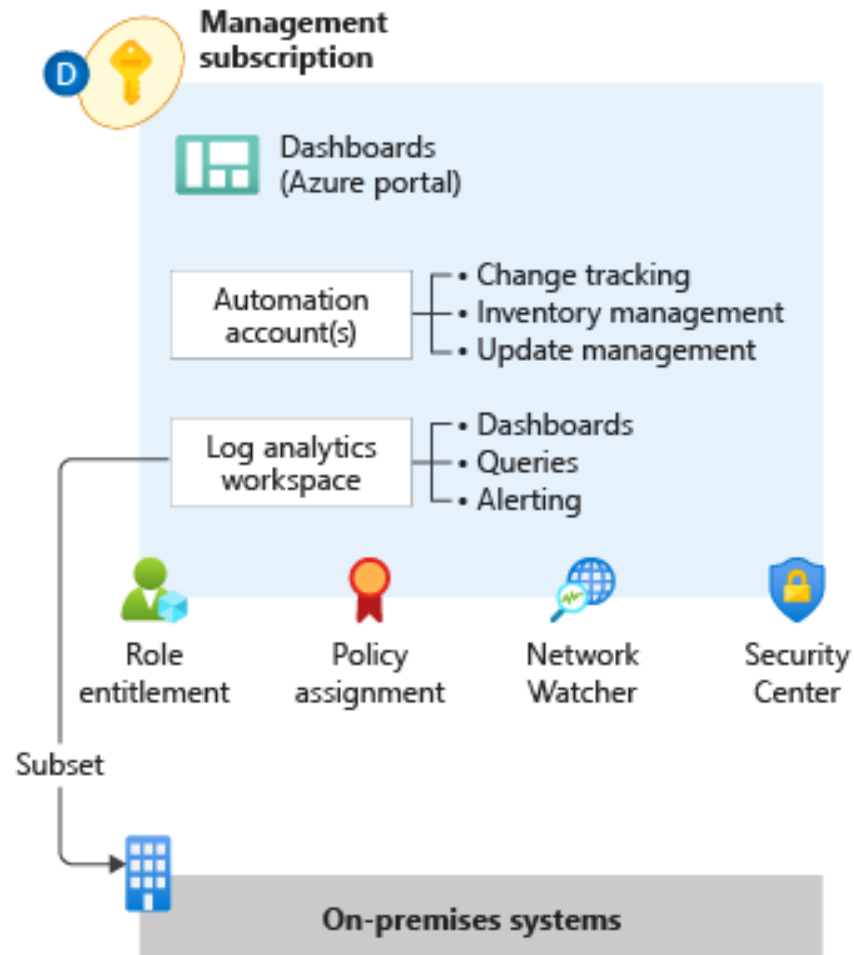
Consider the following design elements:

- ☐ Planning for IP Addressing
- ☐ Configure DNS
- ☐ Define an Azure Networking Topology
- ☐ Azure VWAN (Microsoft Managed)
- ☐ Traditional Azure networking (Customer Managed)
- ☐ Connectivity to Azure



Management (1/2)

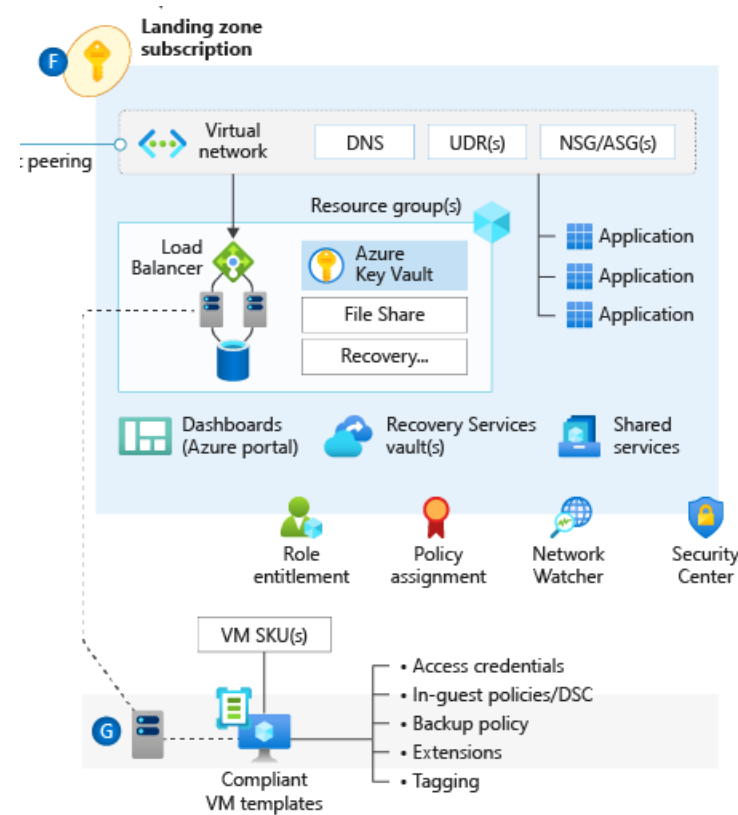
Planning for Platform & Application Management and Monitoring



- ❑ **Log Analytics workspace** is an administrative boundary for security audit logging and achieving a horizontal security lens across the entire customer Azure estate
- ❑ **Azure data retention thresholds** and requirements for archiving



Management (2/2)



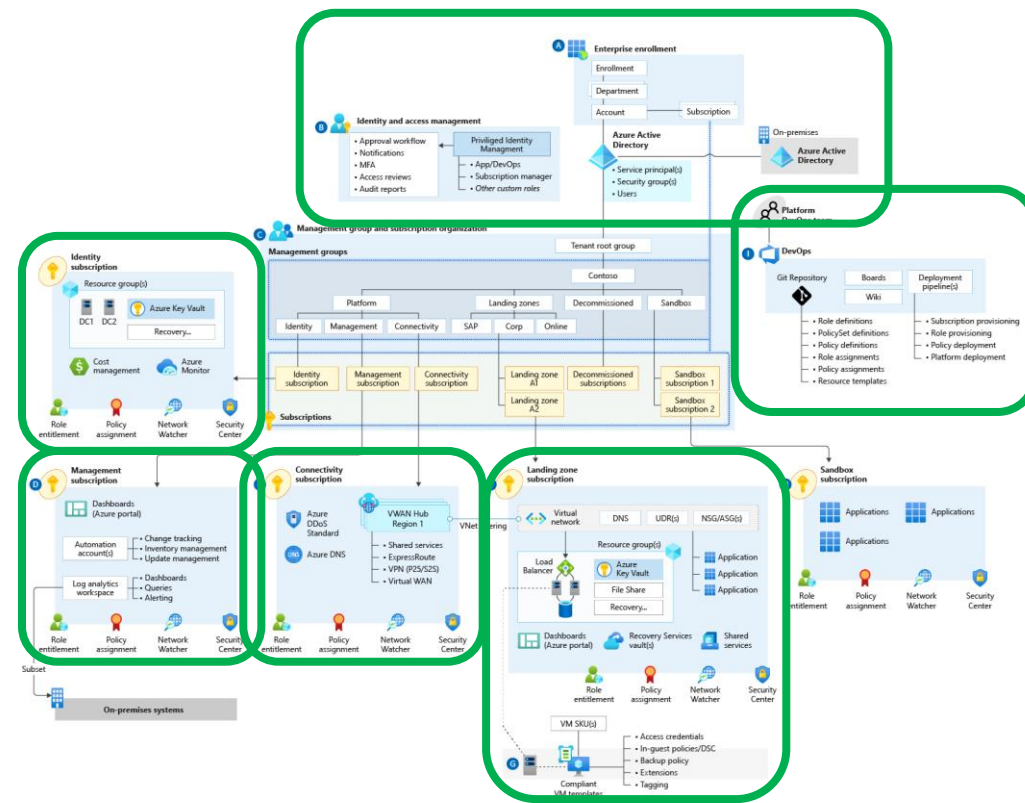
Planning for BCDR

Application and data availability requirements:

- ☐ **BCDR for PaaS** services and the availability of native DR and HA features
- ☐ Support for **multi-region deployments** for failover purposes
- ☐ Application operations with **reduced functionality or degraded performance** in the presence of an outage



Security



Security operations and Access control designs recommendations

- ❑ Premium SKU Key Vault serves a security boundary since access permissions for keys, secrets and certificates are at the vault level
- ❑ can be leveraged where HSM protected keys are required

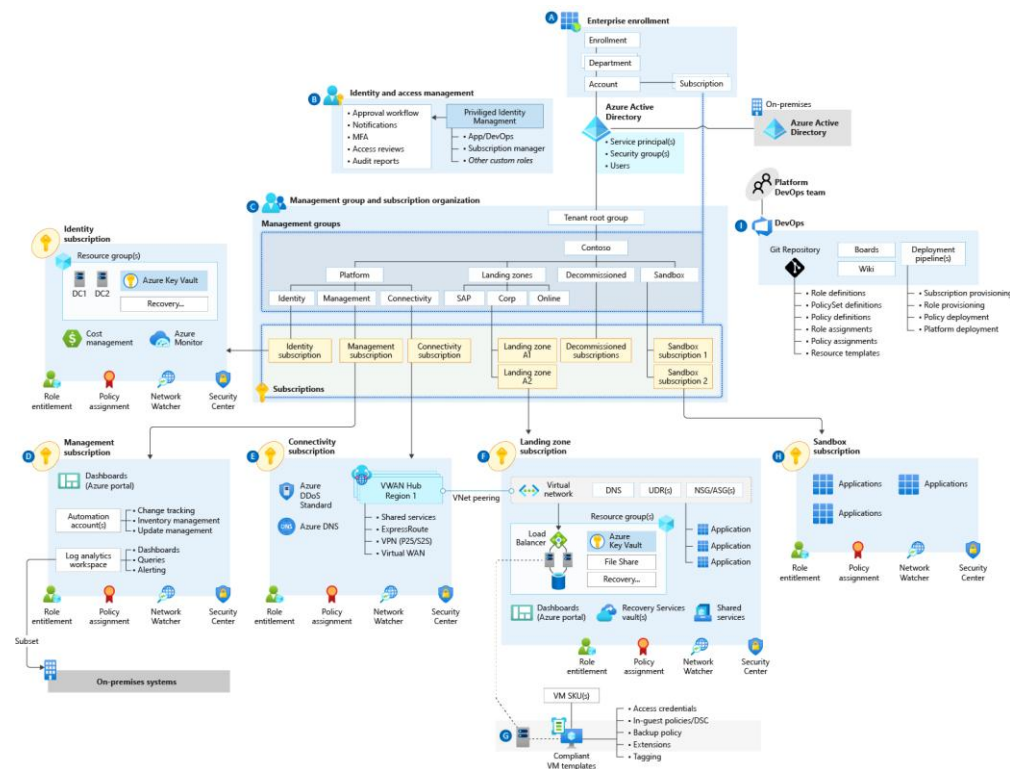
Key rotation and secret expiration

- ❑ Use a federated Key Vault model to avoid transaction scale limits
- ❑ Establish an automated process for key and certificate rotation

Azure Security Benchmark



Governance



Cost Management

- ❑ Best practices for cost reporting and control techniques

Security baseline

- ❑ Guidance and recommendations aligned to the Secure methodology and Security design area

Resource consistency

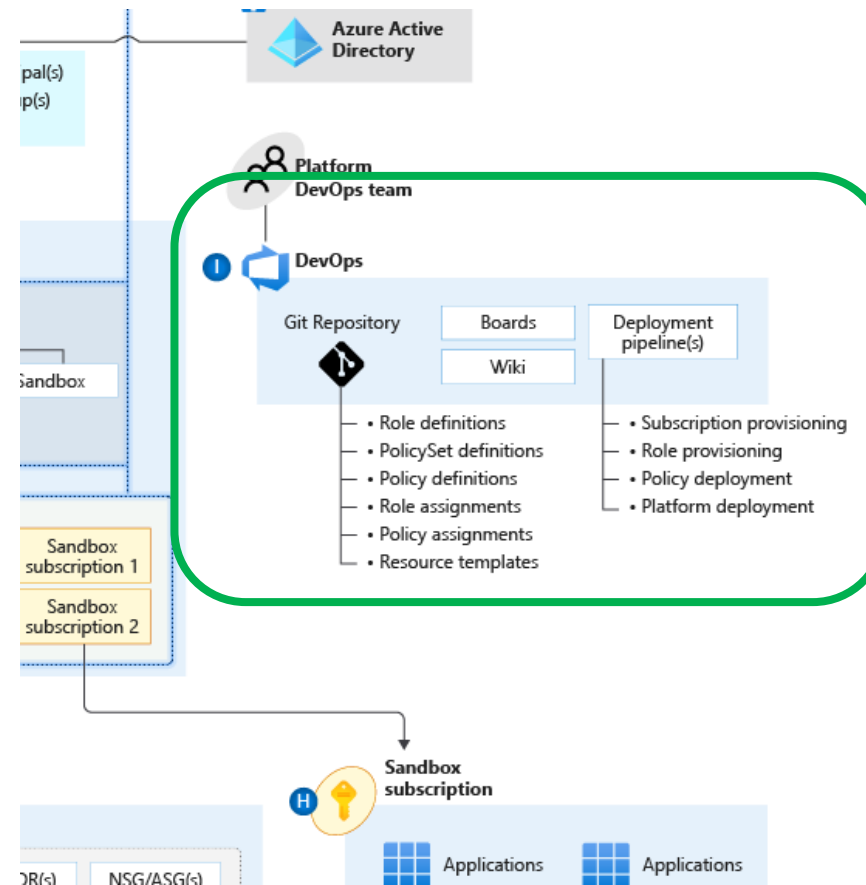
- ❑ Guidance for naming and tagging resources in the environment

Governance and compliance of an Azure landing zone environment



Platform Automation & DevOps

Planning for a DevOps Approach



- ❑ Where central teams are concerned, CI/CD pipelines should be used to manage policy definitions, role-definitions, policy assignments, and template galleries

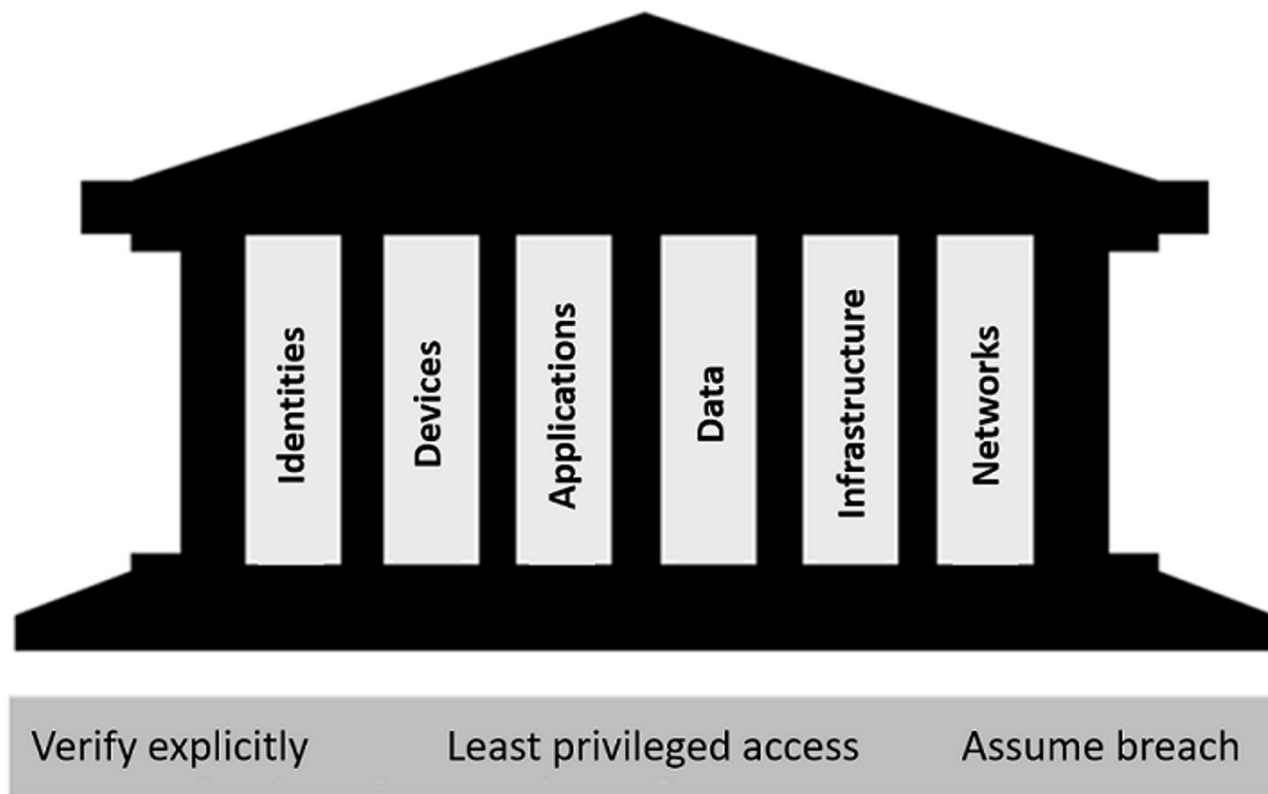
The blanket application of a DevOps model will not miraculously establish capable DevOps teams.

- ❑ Establish a cross functional **DevOps Platform Team** to build, manage and maintain your Azure landing zone architecture.

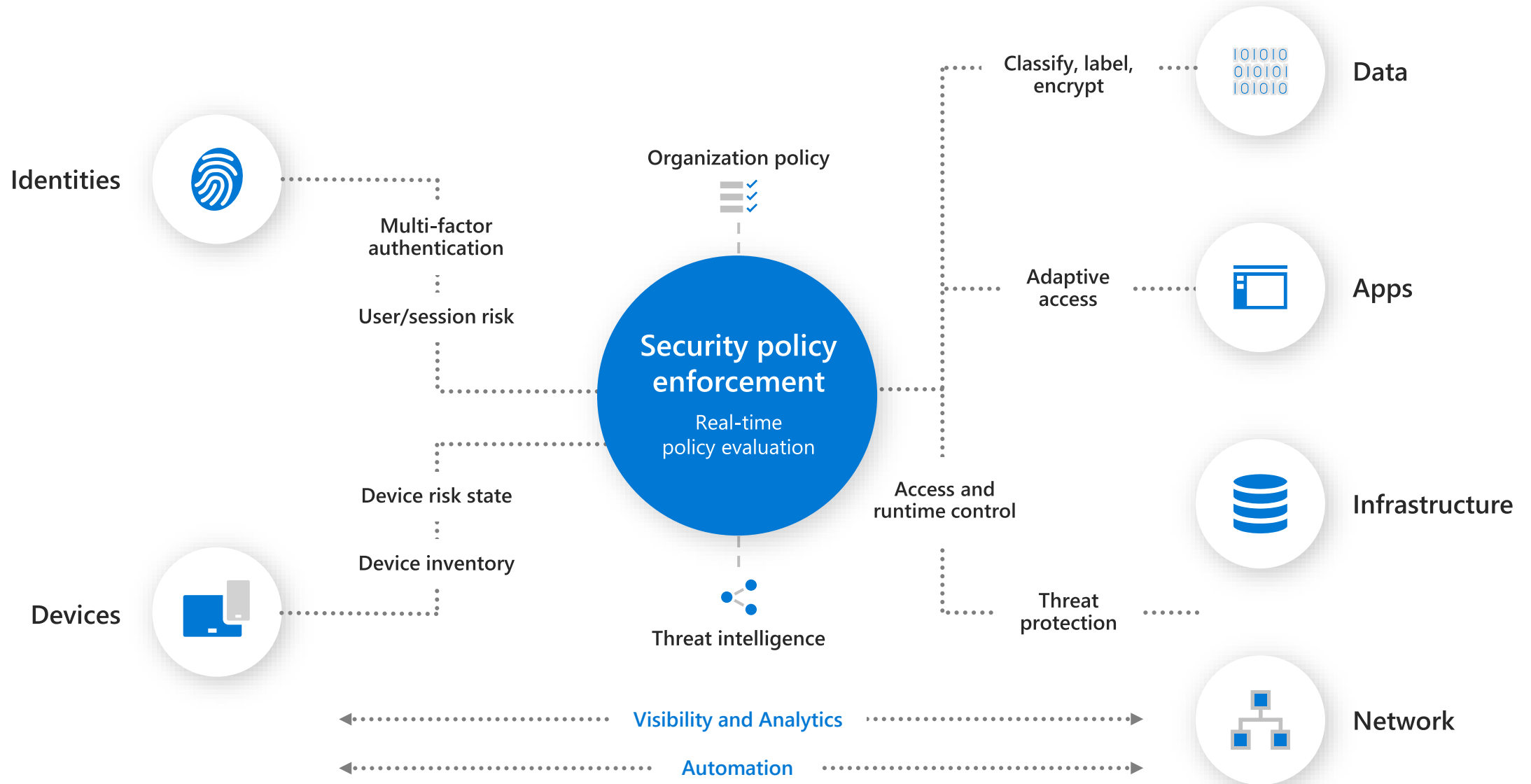
Security and governance

Zero Trust Methodology

“Trust no one, verify everything”



Microsoft Zero Trust architecture



Cloud Data Integrity and Compliance | Microsoft Trust Center



Trust Center

Security

Privacy

Compliance

Products and services

Tools & Documentation

All Microsoft

We're helping

Compliance Overview

Compliance Offerings

Regional and country compliance

European Digital Resilience

EU AI Act

Cloud Services Due Diligence Checklist

Accessibility

Act while fostering responsible AI innovation. [Learn more >](#)

×

TRUST CENTER

Secure and privacy in the age of AI

Microsoft enables trustworthy AI by prioritizing security, privacy, and safety. Learn more about the commitments we've made to ensure your data is safeguarded, our practices are transparent, and your rights are protected.

[Read the blog >](#)

[Watch the video >](#)

Service Trust Portal Home Page

Service Trust Portal

Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.



Certifications, Regulations and Standards



ISO/IEC

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)



SOC

System and Organization Controls (SOC) 1, 2, and 3 Reports



GDPR

General Data Protection Regulation



FedRAMP

Federal Risk and Authorization Management Program



PCI

Payment Card Industry (PCI) Data Security Standards (DSS)



CSA Star

Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)



Australia IRAP

Australia Information Security Registered Assessors Program (IRAP)



Singapore MTCS

Multi-Tier Cloud Security (MTCS) Singapore Standard



Spain ENS

Spain Esquema Nacional de Seguridad (ENS)

Reports, Whitepapers and Artifacts



BCP and DR

Business Continuity and Disaster Recovery



Penetration Test and Security Assessments

Attestation of Penetration tests and security assessments conducted by third parties



Privacy and Data Protection

Privacy and Data Protection Resources



FAQ and Whitepapers

Whitepapers and answers to frequently asked questions



AI Resources

Resources describing the approach to Compliance, Security and Privacy in the AI solutions such as Copilot and Azure Open AI

Industry and Regional Resources

Azure compliance documentation

If your organization needs to comply with legal or regulatory standards, start here to learn about compliance in Azure.

Compliance offerings

Global

- 📖 CIS benchmark
- 📖 CSA STAR Attestation
- 📖 CSA STAR Certification
- 📖 CSA STAR self-assessment
- 📖 SOC 1
- 📖 SOC 2
- 📖 SOC 3

Global

- 📖 ISO 20000-1
- 📖 ISO 22301
- 📖 ISO 27001
- 📖 ISO 27017
- 📖 ISO 27018
- 📖 ISO 27701
- 📖 ISO 9001
- 📖 WCAG

US government

- 📖 CJIS
- 📖 CMMC
- 📖 CNSSI 1253
- 📖 DFARS
- 📖 DoD IL2
- 📖 DoD IL4
- 📖 DoD IL5
- 📖 DoD IL6
- 📖 DoE 10 CFR Part 810
- 📖 EAR
- 📖 FedRAMP
- 📖 FIPS 140

US government

- 📖 ICD 503
- 📖 IRS 1075
- 📖 ITAR
- 📖 JSIG
- 📖 NDAA
- 📖 NIST 800-161
- 📖 NIST 800-171
- 📖 NIST 800-53
- 📖 NIST 800-63
- 📖 NIST CSF
- 📖 Section 508 VPATs
- 📖 StateRAMP

Financial services

- 📖 23 NYCRR Part 500 (US)
- 📖 AFM and DNB (Netherlands)
- 📖 AMF and ACPR (France)
- 📖 APRA (Australia)
- 📖 CFTC 1.31 (US)
- 📖 EBA (EU)
- 📖 FCA and PRA (UK)

Financial services

- 📖 FINRA 4511 (US)
- 📖 FISC (Japan)
- 📖 FSA (Denmark)
- 📖 GLBA (US)
- 📖 KNF (Poland)
- 📖 MAS and ABS (Singapore)
- 📖 NBB and FSMA (Belgium)

Financial services

- 📖 OSPAR (Singapore)
- 📖 PCI 3DS
- 📖 PCI DSS
- 📖 RBI and IRDAI (India)
- 📖 SEC 17a-4 (US)
- 📖 SEC Regulation SCI (US)
- 📖 SOX (US)

Healthcare and life sciences

- 📖 ASIP HDS (France)
- 📖 EPCS (US)
- 📖 GxP (FDA 21 CFR Part 11)
- 📖 HIPAA (US)
- 📖 HITRUST
- 📖 MARS-E (US)
- 📖 NEN 7510 (Netherlands)

Azure status

Azure status

This page is only used for widespread incidents.



[Sign in to view incidents that may be affecting your services](#)

[Go to Azure Service Health >](#)

HELPFUL LINKS

Azure status history

[Learn when we use this page](#)

Get notified of outages that impact you

Building reliable applications on Azure

Updated 39 seconds ago | Refresh every 2 minutes

 Good
 Information
 Warning
 Critical
 -- N/A

[illegible]

Microsoft Privacy Statement

Last Updated: May 2025

[What's new?](#)



Print

Expand All Collapse All

Microsoft Privacy Statement

[Personal data we collect](#)

[How we use personal data](#)

[Reasons we share personal data](#)

[How to access and control your personal data](#)

[Cookies and similar technologies](#)

[Products provided by your organization—notice to end users](#)

[Microsoft account](#)

[Collection of data from children](#)

[Other important privacy information](#) >

Product-specific details:

[Artificial Intelligence and Microsoft Copilot capabilities](#)

[Enterprise and developer products](#) >

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Young people may prefer starting with the [Privacy for young people](#) page. That page highlights information that may be helpful for young people.

For individuals in the United States, please refer to our [U.S. State Data Privacy Notice](#) and the [Consumer Health Data Privacy Policy](#) for additional information about the processing of your personal data, and your rights under applicable U.S. state data privacy laws.

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use, and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices you make, including your privacy settings and the products and features you use. We also obtain data about you from Microsoft affiliates, subsidiaries, and third parties.

SLAs for Azure products and services

- Three key characteristics of SLAs for Azure products and services:
 - Performance targets, uptime and connectivity guarantees: Uptime or connectivity rates, such as availability
 - Performance targets range: Typical SLAs specify performance-target commitments ranging from 99.9 percent (*three nines*) to 99.99 percent (*four nines*)
 - Service credits: Percentage of the applicable monthly service fees credited to you if a service fails to meet ALS uptime guarantee
- For more information about specific Azure SLAs for individual products and services, see [Service Level Agreements](#)



CSP



What is CSP?

- Cloud Solution Provider (CSP) is a program, that helps Microsoft partners to be more involved with their customers' business, beyond just reselling licenses.
- CSP partners can transact across Microsoft cloud services (i.e., Azure, M365, EMS, D365 etc) through a single platform
- CSP enables partners to own the customer lifecycle and relationship end-to-end; set the price, terms and directly bill customers; directly provision and manage subscriptions; attach value-added services; and be the first point of contact for customer support.



Different CSP models

Direct-bill model (1-tier Cloud Solution Provider):

- In the direct-bill model, partners purchase Microsoft products and subscriptions directly from Microsoft and sell them directly to their customers. The direct-bill model requires partners to sell to, bill, manage, and support their customers

Indirect model (2-tier reseller):

- As an indirect reseller, you can work with indirect providers who can provide the tools and resources to help you manage your customer relationship. With the indirect model, you can purchase from an indirect provider who can collaborate with you for customer support and billing

Partner Role and Permissions

Partner Center Roles	Level of Access
Admin agent	Customer management, View pricing and offers, Subscription management, Request delegated administrator privileges, Administer on behalf of a customer, View and manage Azure spending budgets, View and manage billing, invoices, and reconciliation files
Global admin	View agreements, price lists, and offers, Can access all Microsoft account/services with full privileges, View, create, and manage all partner users, Cancel Azure subscription, View and manage billing, invoices, and reconciliation files
Billing admin	View and manage billing, invoices, and reconciliation files, Manage billing issues on behalf of customers
Sales agent	Request a relationship with a customer, View the customer agreement, View pricing and offers, Manage customer leads

What are AOBO and FPO? Why are they required?

Admin On Behalf Of

- Admin on Behalf of is a privilege that enables users with admin agent roles on the Partner tenant to manage and make purchases on behalf of customers on the Partner Center
- The admin agents get this privilege once the reseller relationship is accepted by the customer

Foreign Principal Object

- This is a user group that is created when an Admin Agent purchases an Azure Subscription under their customer tenant
- It enables partners to manage their customer's subscriptions and services on the Azure Portal
- This user group has the RBAC owner permission on the Azure Subscription

Identity and Eligibility



It is very important to identify who the case creator/requester is and their access level at the billing account or partner tenant level to ensure we share the appropriate data with them. This helps us comply with Microsoft's Data Privacy Policies



The case creator/requester could either be a partner/indirect provider/indirect reseller/customer. Each of them have different user roles on either the partner tenant or the customer tenant and each role has its own access/permission level



Since the Admin agents and the Global admins on the partner tenant have access to manage customer's subscription and billing, these users only can approve cancellations and sharing of billing information with end customer



Any other user may request for billing information or cancellation, but do not share any cost information or perform cancellations without the approval of an admin agent or a global admin. You may share the consumption information only with the end customer.



NOTE: Be careful while sharing the billing or consumption information. Share information only for that customer and not of all other customers

Partner Access Issues

Partner unable to access customer's Azure subscription and services on Azure Portal

Step 1: Identity and eligibility

- The requester should either be a Direct Partner (tier 1) or an Indirect Provider
- The requester should have admin agent role on the partner tenant

Step 2: Correct Tenant

- If partner wants to access a customer's CSP subscription then they need to be logged into the correct customer tenant on the Azure Portal and not their partner tenant

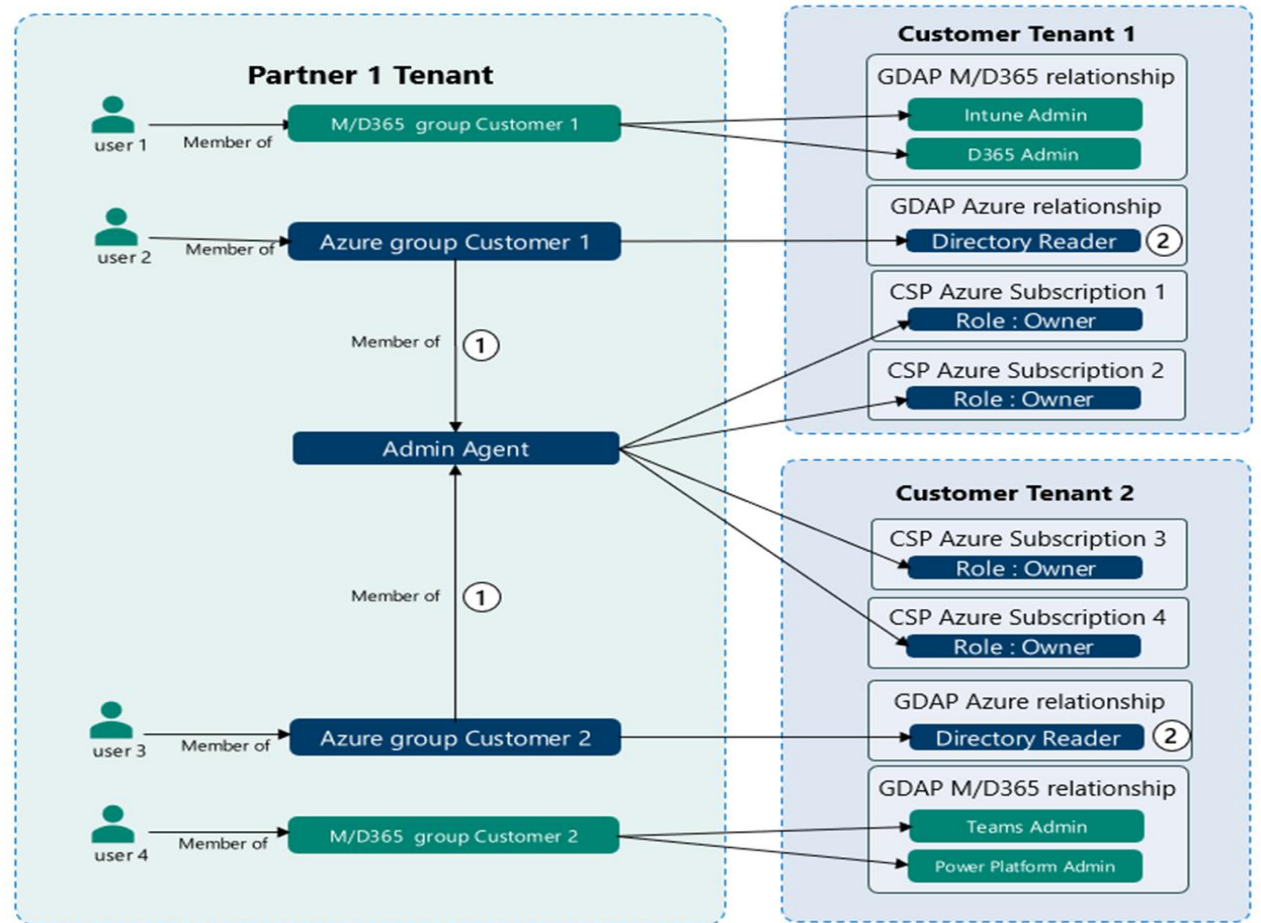
Step 3: Can user access CSP?

- Run this check on ASC
- If partner is added as a guest user in customer tenant, then the admin agent cannot access subscription on Azure Portal. The customer would have to remove the admin agent's email from their tenant
- If the FPO role is removed, then admin agents cannot access the subscription on Azure Portal. Please have the partner and end customer follow instructions in [Reinstate admin privileges for Azure CSP - Partner Center | Microsoft Learn](#)

ASMS Common Support Scenarios..

Step 1: Partner unable to see the subscription in the Azure Portal...

- GDAP:
<https://learn.microsoft.com/en-us/partner-center/customers/gdap-introduction>
- Someone with the *Admin agent* role at a partner organization can [create a GDAP relationship request](https://learn.microsoft.com/en-us/partner-center/customers/gdap-faq). The maximum duration of a GDAP relationship is two years.
<https://learn.microsoft.com/en-us/partner-center/customers/gdap-faq>

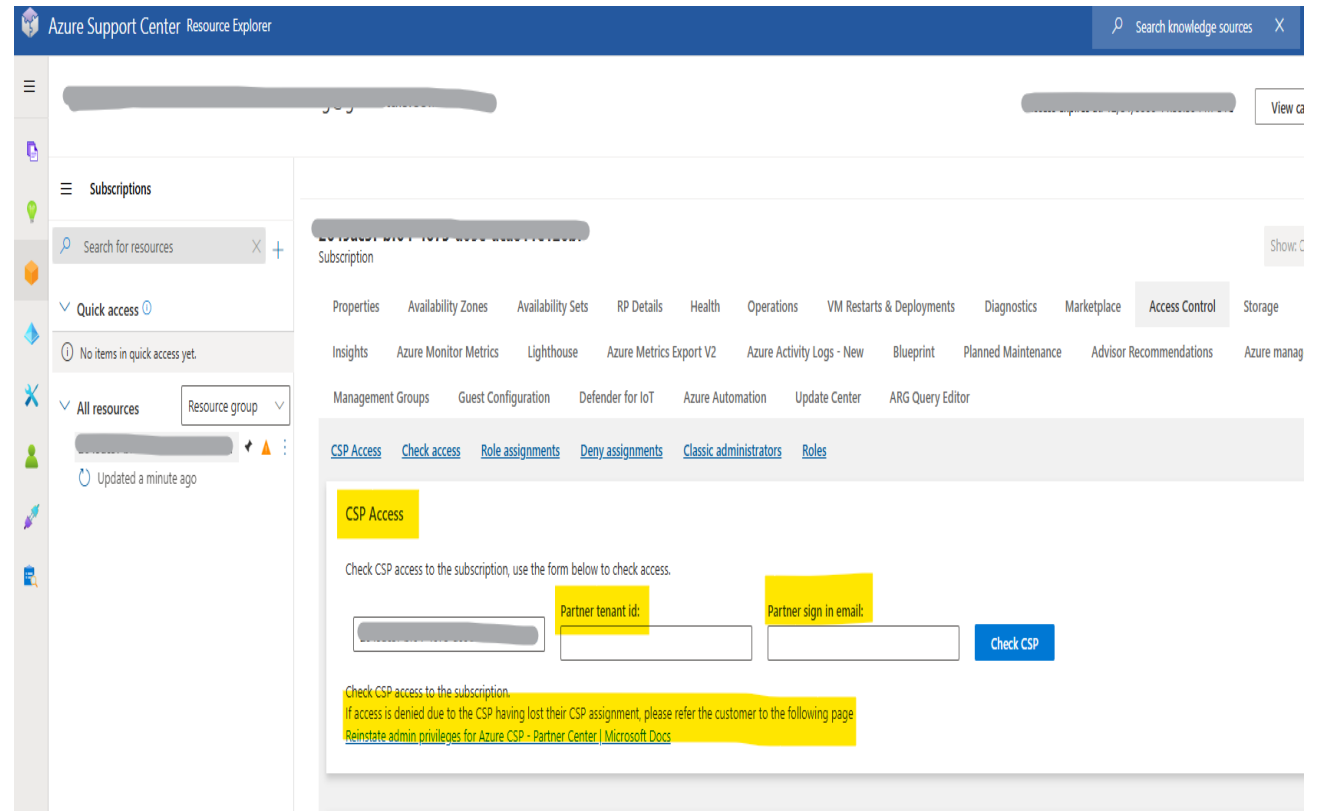


ASMS Common Support Scenarios..

Step 3: Partner unable to see the subscription in the Azure Portal...

- When CSP Admin access is removed.
- Can be fixed by reinstating Admin privileges for subscription:

<https://learn.microsoft.com/en-us/partner-center/customers/reinstate-csp>





Subscription Ownership Transfer

- Subscription Ownership Transfer can be performed from one partner tenant to another only. A CSP (legacy/new commerce) subscription cannot be transferred from one customer tenant to another. This process is customer self-serve, where all involved parties have specific actions to be completed
[Transfer Azure subscriptions, reservations, or savings plans \(under an Azure plan\) to another CSP partner - Partner Center | Microsoft Learn](#)
- EA subscriptions can be transferred to CSP and this is also a self-serve. However, this is out of support scope for Delivery Partners, we transfer all legacy EA cases to EA team as per the instructions in the TSG: [ASMS – Sales Motion and Support Entitlement Handling \(microsoft.com\)](#)
- CL/MOSP subscriptions cannot be transferred to CSP (Legacy/New Commerce)
- Legacy CSP to New Commerce CSP within same partner tenant is self-serve
[Move customers from current Azure offers to Azure plan - Partner Center | Microsoft Learn](#)
- Legacy CSP to New Commerce CSP to different partner tenant not possible
- FL to New Commerce CSP self-serve
[Transfer Azure product billing ownership to your Microsoft Partner Agreement \(MPA\) - Microsoft Cost Management | Microsoft Learn](#)



ACM for Partners and Customer

- **Partners:** ACM is natively available only for new commerce subscriptions (PL), for all global admins and admin agents on the partner (direct partner/indirect provider) tenant. The partner can access costs for all their customers in ACM. Apart from the partner centre roles, partners with appropriate modern billing roles (BGO, Billing Profile Owner/Contributor, Invoice Manager) can also access ACM
- **Customers:** Partner Led customers cannot access costs for their PL subscriptions on ACM by default, unless their partner/indirect provider enables ACM for the customer from partner centre. Once ACM is enabled for customer, users with appropriate RBAC roles on the subscription will have access to subscription costs on ACM
- [Get started with Cost Management for partners - Microsoft Cost Management | Microsoft Learn](#)

Home > Cost Management > Billing - Billing accounts > <BillingAccount> - Customers

<BillingAccount> - Customers

Search (Ctrl+/)

Overview

Cost management

Cost analysis

Budgets

Billing

Invoices

All transactions

Reservation transactions

Customers

Recurring charges

Azure subscriptions

Billing profiles

Settings

View charges for customers that have accepted Microsoft Customer Agreement. The list shown below doesn't include customers that haven't accepted Microsoft Customer Agreement but have Azure Reservations and Marketplace products. However, the Azure Reservations and Marketplace charges for these customers show up on the invoice, transactions and in the billing profile's monthly charges. To view all other customers, go to the [Microsoft partner center](#).

Search

Search by customer name

NAME	MONTH-TO-DATE C...	LAST MONTH'S CHA...
0729TestUKCustomer	GBP 130.14	0.00
0730TestModernCustomer	GBP 37.01	GBP 49.76
0801TestUKModernCustomer	0.00	0.00
Camila PAL testing	GBP 50.94	GBP 150.11
Contoso	0.00	0.00
ContosoTestTest	0.00	0.00
Johnny Modern Cust DE1	EUR 35.58	EUR 100.16
Johnny Modern Cust DE2	EUR 30.27	EUR 86.88

Home > Cost Management > Billing - Billing accounts > <BillingAccount> - Customers > 0729TestUKCustomer - Policies

0729TestUKCustomer - Policies

Customer

Search (Ctrl+/)

Save Discard

Overview

Cost management

Cost analysis

Budgets

Billing

All transactions

Azure subscriptions

Recurring charges

Settings

Transfer requests

Policies

Users in 0729TestUKCustomer with access to an Azure subscription can view its charges at pay-as-you-go price.

Yes No



Partner Earned Credits

- In the legacy CSP, partners were billed at discounted rates and this discount was termed as Partner Margin
- With CSP transitioning to New Commerce and all subscriptions getting billed at Pay-As-You-Go rates, the Partner Margin was replaced by Partner Earned Credits (PEC) for services managed under the new Azure Plan. PEC will be at a fixed rate of 15%

Pre-Requisites for getting Partner Earned Credits

- The partner must have an active Microsoft AI Cloud Partner Program (formerly known as MPN) agreement and a valid role-based access control (RBAC).
- The partner must have access permissions to the subscription, which can be set in one of the three ways below
 - **Admin on behalf of (AOBO)** is the default. When a partner establishes a reseller relationship with their end customer AOBO is set up and this enables the partner to provisions an Azure Plan subscription for a customer, AOBO is set in the form of a **foreign principal** that inherits owner permissions on the Azure subscription. The AOBO permissions mean that Admin Agents group - inherit these permissions.
 - **Azure Lighthouse** is an option for partners interested in enabling sophisticated cross-tenant management experience for Azure solutions
 - **Individual user accounts and service principals (RBAC)**: Sometimes it is best to work with individual user accounts that have permissions to Azure subscriptions via PAL association