Course Overview

Matthew Ulasien
Azure Training Architect

AZ-900 Preparation Info

Course #3 in preparation track

Recommend doing prep courses in order

Course Overview

Core Azure Architecture and Services

Physical and Organizational structure

Compute/Networking/Storage

- Power plant for all Azure solutions

Azure Regions

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Azure Regions

- Understanding Regions
- How to Choose a Region
- Region Pairs
- Sovereign Regions

Matthew Ulasien
Azure Training Architect

Understanding Regions: The Big Question

‘Where’ is Azure?

How is it physically organized?

Understanding Regions: Microsoft's Definition

"A **region** is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network."

Definition from Microsoft documentation

Understanding Regions: Simple Definition

Geographically distributed groups of datacenters

Region = Two or more data centers, not too far from each other, connected with a high-speed connection

Note: Some regions only have single datacenter (more on this later)

Multiple regions strategically located worldwide

Azure Regions

Understanding Regions: Global Distribution

60+ regions and counting!

Understanding Regions: Connectivity

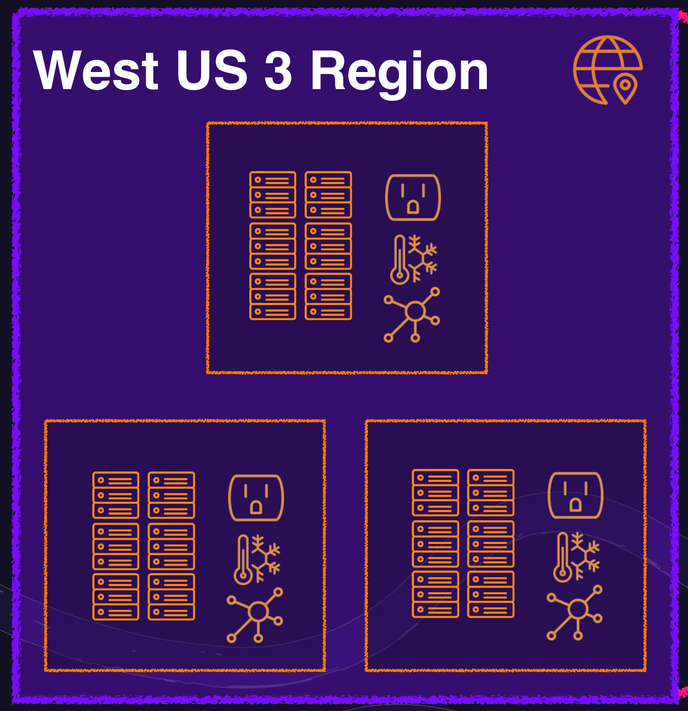
Private Global Fiber Network

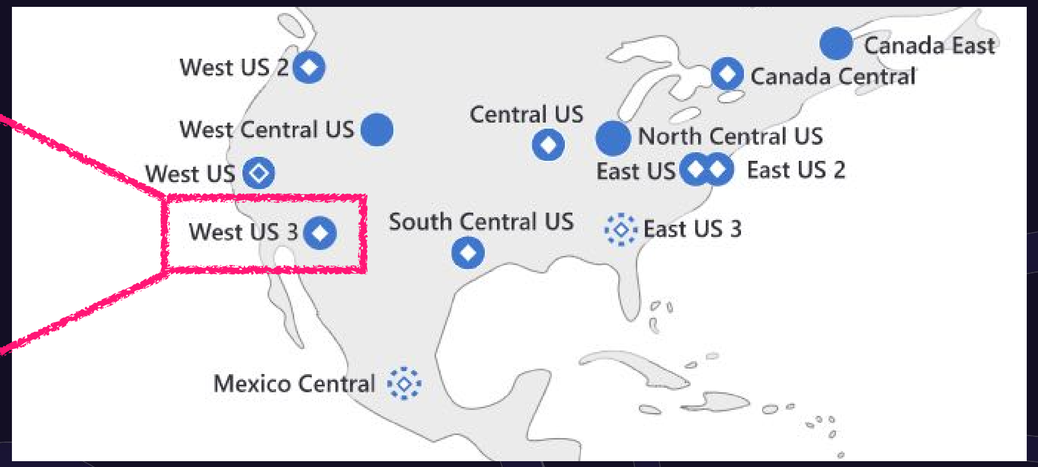
Understanding Regions: Example (West US 3)

Multiple nearby datacenters

Each datacenter is independent from each other

- Power, cooling, networking





How to Choose a Region

You can select the region for deploying Azure resources

Location

Choose a region closest to your users to minimize latency.

Features

Some features aren't in all regions. If you need a specific feature, some regions might be unavailable.

Price

The price of services varies from region to region.

You will often have to choose which is the most important: location, features, or price.

Region Pairs

Two closely linked regions for redundancy

1. **Each Region Is Paired**

   All (except Brazil South) are paired within the same geographic area, at least 300 miles apart.

2. **Outage Failover**

   If the primary region has an outage, you can fail over to the secondary region.

3. **Planned Updates**

   Only one region in a pair is updated at any one time.

4. **Replication**

   Some services use paired regions for replication.

Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe

Sovereign Regions

Isolated regions ensuring government compliance within specific jurisdictions

- Not part of Azure public cloud
- Approval required to join
- Not all services available

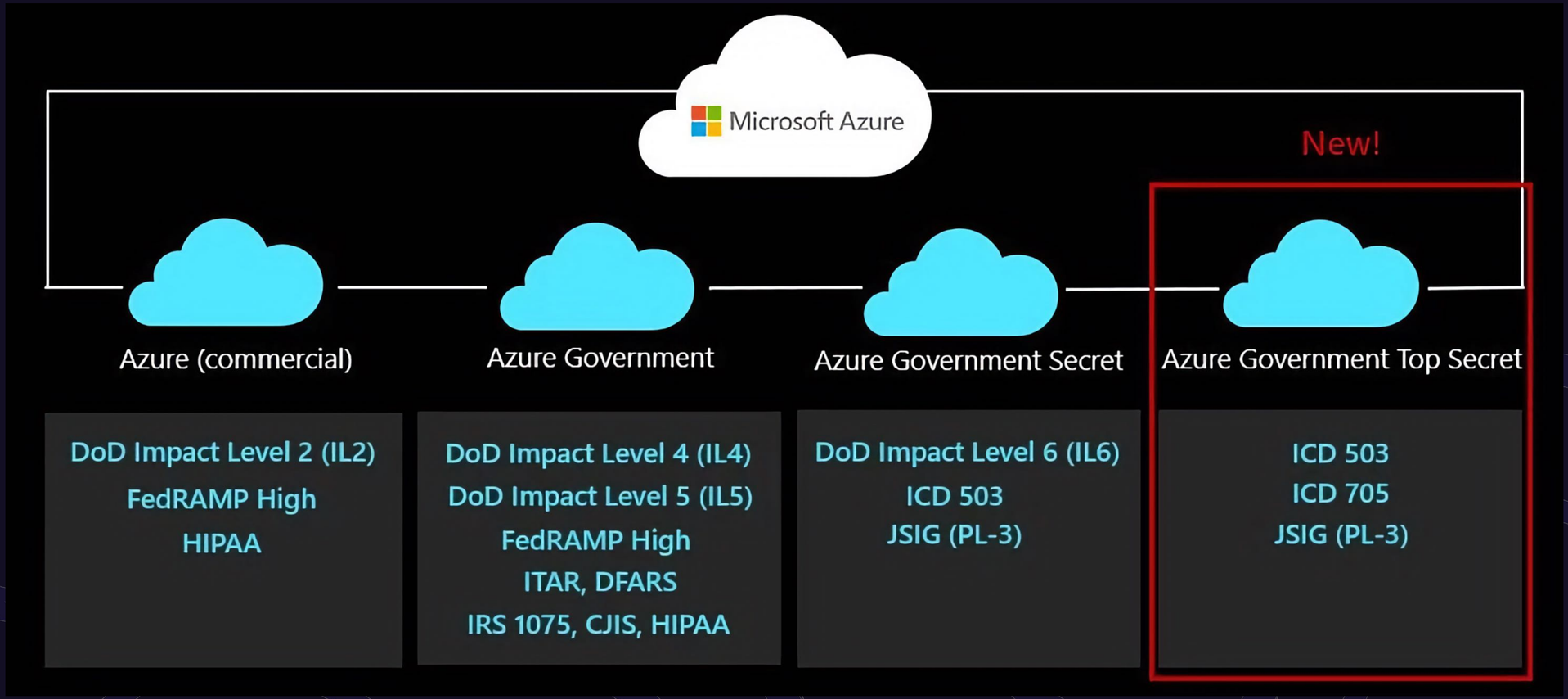
Azure for US Government

Azure China

Sovereign Regions: Azure for US Government

Meets higher compliance requirements

A cloud for mission across data classifications



Sovereign Regions: Azure for US Government Eligibility

US government entity or solutions provider

Federal, state, local, or tribal governments

Government contractors

Sovereign Regions: Azure China

Isolated regions required for Azure workloads in China

- Operated by third-party provider (21Vianet)
- Data stays in China’s datacenter to ensure compliance
- Requires business presence in China

Summing It Up

Regions

- Geographically distributed physical infrastructure
- Multiple nearby datacenters in each region

Region Pairs

- Linked regions in same geographic area
- Redundancy/replication

Sovereign Regions

- Isolated/private regions in US/China
- Requirements to join
- Meet compliance requirements

Availability Zones

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Availability Zones

- What Are Availability Zones?
- Visual Representation
- Regional Availability
- Using Availability Zones

Matthew Ulasien
Azure Training Architect

What Are Availability Zones?

Physically separate datacenters within an Azure region

Physical Location

Each availability zone is a physical location within a region.

1+ datacenters per zone

Independent

Each zone has its own power, cooling, and networking.

High availability

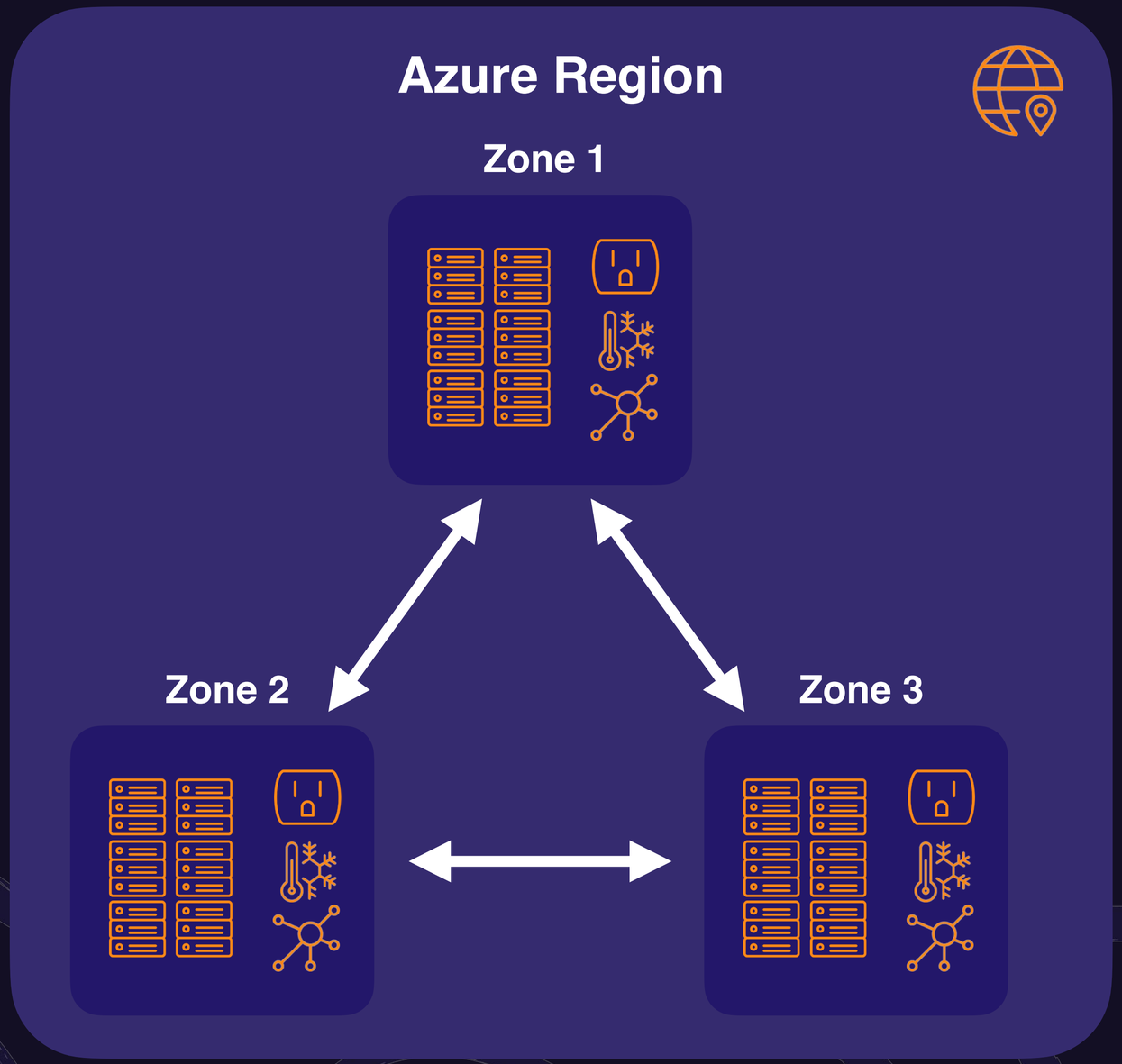
Zones

Minimum of three zones

Not available in all regions

Availability Zones

Visual Representation



2 ms latency round trip between zones (i.e., within a few miles/km)

Regional Availability

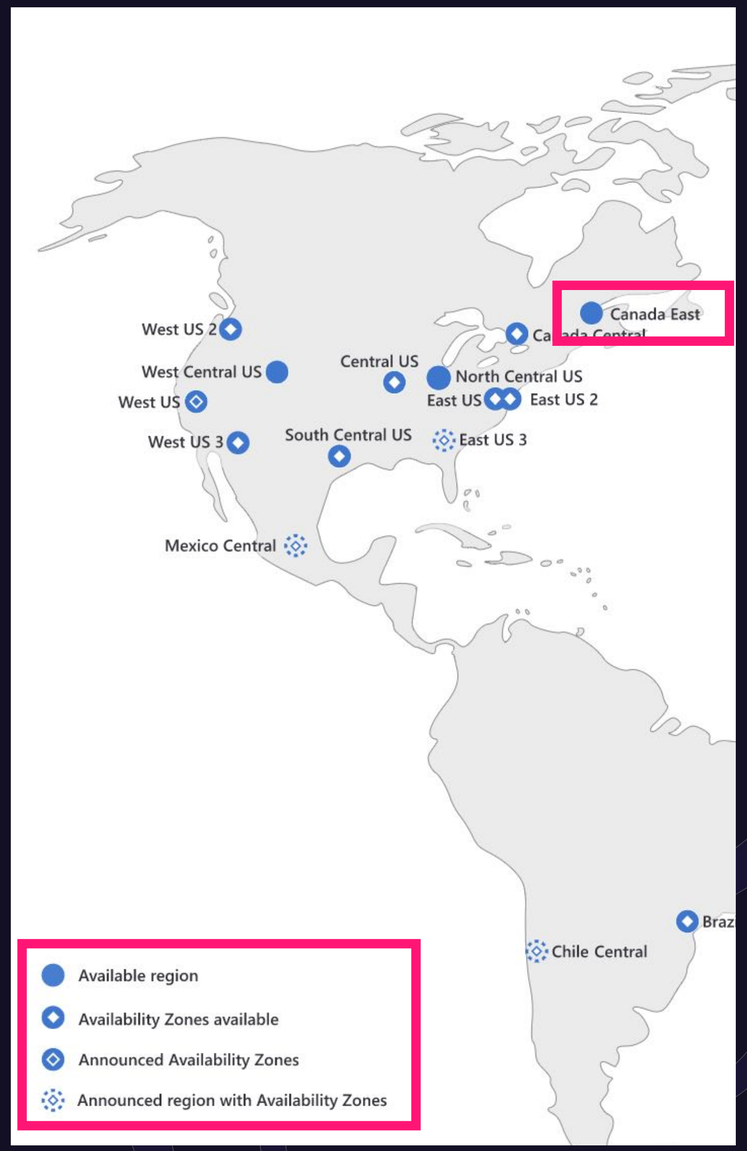
Not all regions have availability zones

At least one zone-enabled region per country with Azure presence

More zone availability becoming available

Regions	Canada Central Start free >	Canada East Start free >
LOCATION	Toronto	Quebec City
YEAR OPENED	2016	2016
AVAILABILITY ZONES PRESENCE	Available with 3 zones	Nearest region with zones available: Canada Central

West US Start free >
California
2012
Coming soon



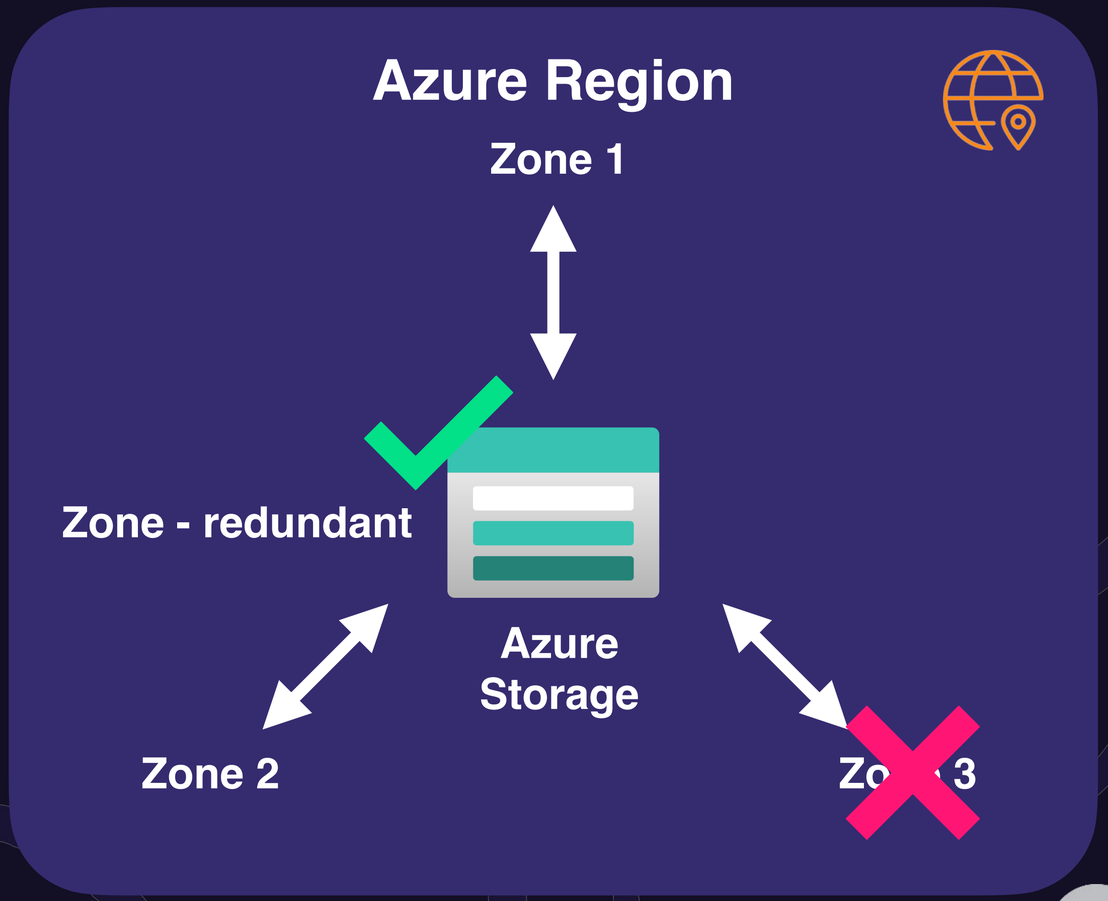
Using Availability Zones

Goal: Redundancy within a region

Solution/service replicated across multiple zones

If one zone goes down, service still operational

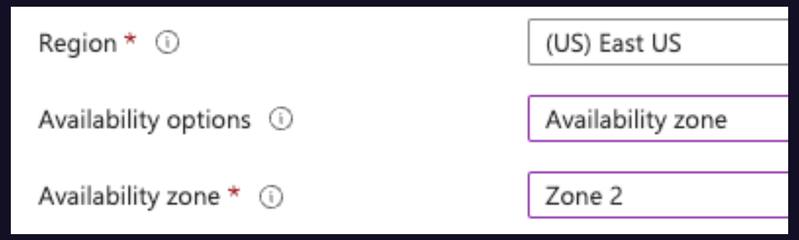
Essential for adding redundancy to your application



Methods of using Availability Zones

Zonal services:

- You associate a resource with a specific zone
- Example: Deploy VM to Zone 2



Zone-redundant services

- Service automatically replicates across zones
- Example: Zone-redundant storage account

Be aware: Duplicating services across zones has additional costs.

Summing It Up

Availability Zones: The Big Idea

- Isolated, independent datacenters in a single Azure region

All about redundancy

- If one zone is unavailable, others still available
- Design application/services to take advantage of multiple zones

Exploring Azure Global Infrastructure

Matthew Ulasien
Azure Training Architect

Demo

Explore Microsoft's interactive infrastructure maps

- Explore regions, network links, and more

https://datacenters.microsoft.com

Resource Organization

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Resource Organization

Resource Organization at a Glance

Resources

Resource Groups

Subscriptions

Management Groups

Matthew Ulasien

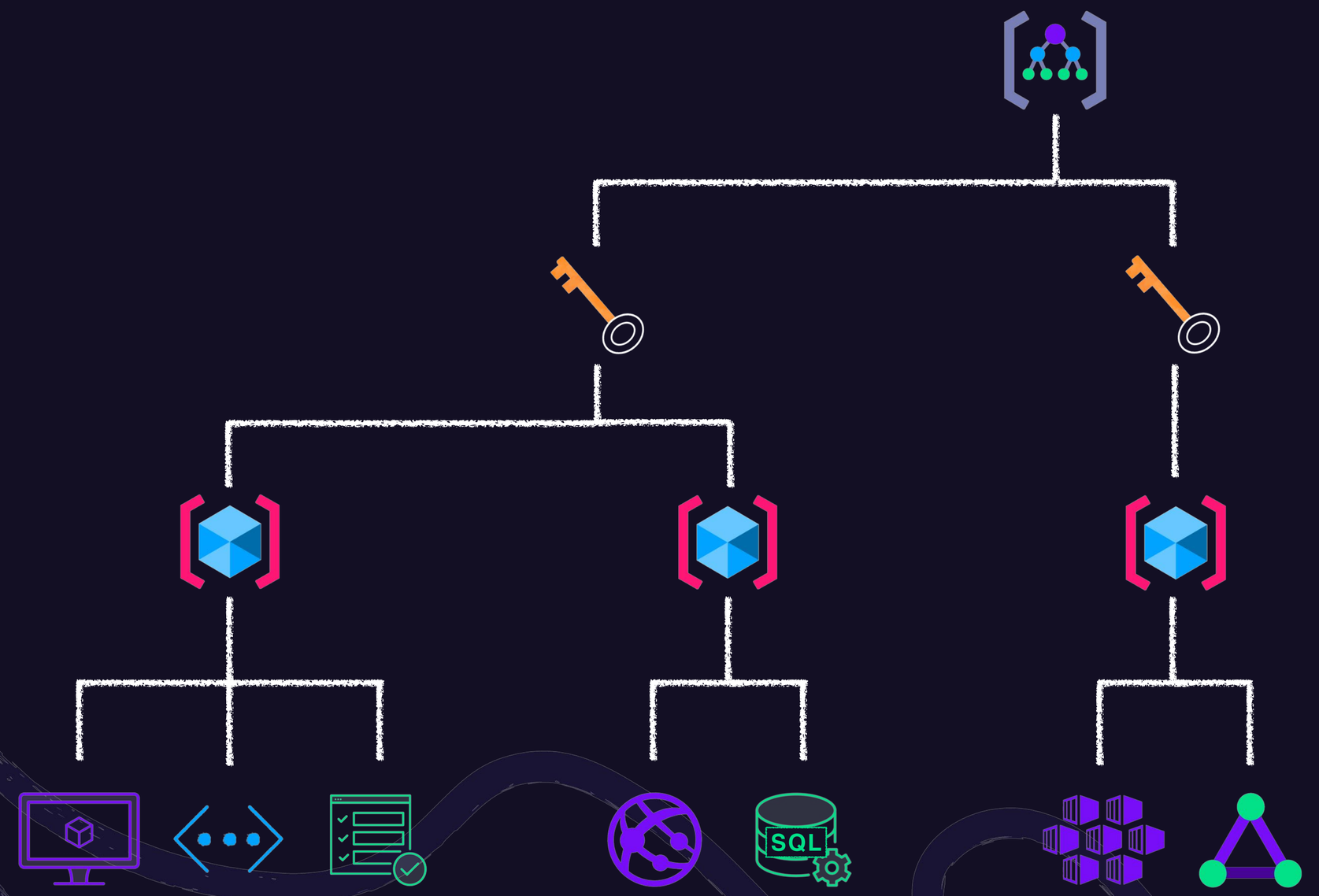
Azure Training Architect

Resource Organization at a Glance

Management Infrastructure

How do we manage and organize all our Azure ‘stuff’?

Resource Organization at a Glance



Management Groups

Subscriptions

Resource Groups

Resources

Resources

- Basic building blocks
- Anything you create is a resource
- (Usually) assigned to a region
- Every resource has a name
- Most resources have a cost

Resource Organization

Resource Groups

Resource Group

Resource Group

Resource Group

Resource Groups

- Groupings of resources
- All resources must be in a resource group
- Group resources with the same lifecycle/access control needs

Resource Groups: Quick Facts

1. **One Resource**
   Each resource can only exist in a single resource group.

2. **Add/Remove**
   You can add or remove resources to any resource group at any time.

3. **Move Resource**
   You can move a resource from one resource group to another.

4. **Multiple Regions**
   Resources from multiple regions can be in one resource group.

5. **Access Control**
   You can give users access to a resource group and everything in it.

6. **Interact**
   Resources can interact with other resources in different resource groups.

7. **Location**
   A resource group has a location, or region, as it stores meta data about the resources in it.

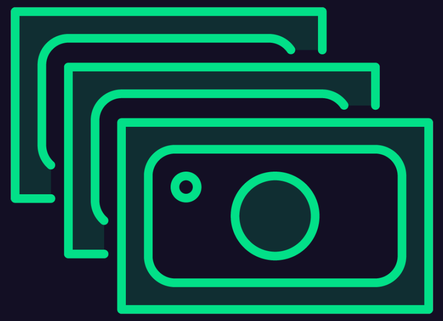
Resource Group: Flexibility

No hard rules

Organize in a way that’s useful to you

Subscriptions

Management, access, and billing boundary



Management

All resources/resource groups belong in a subscription.

Access Control

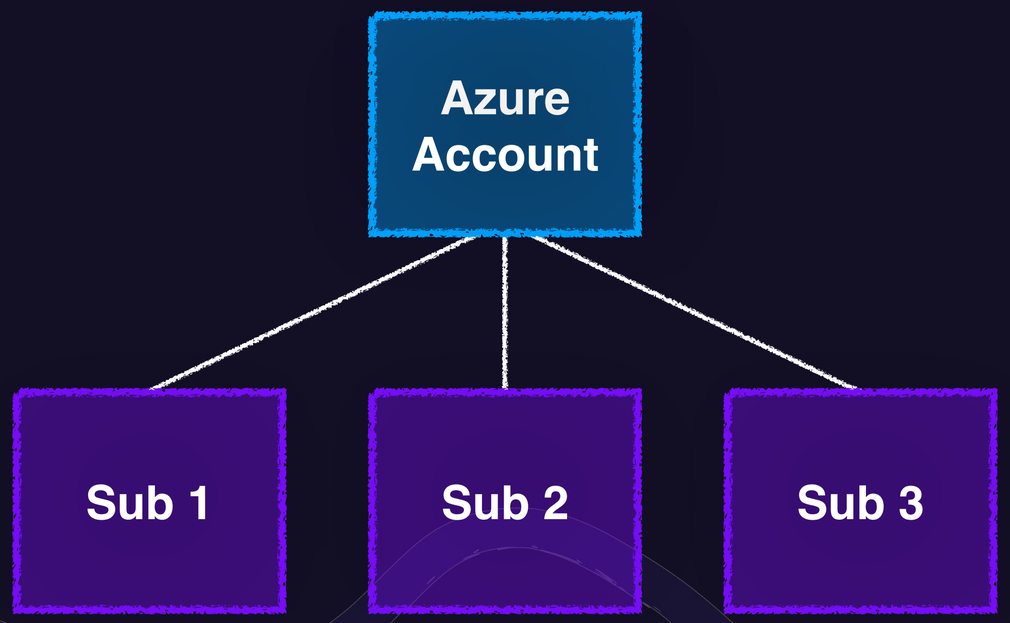
User accounts/permissions granted to subscription.

Billing

Payment method associated with subscription.

Subscriptions

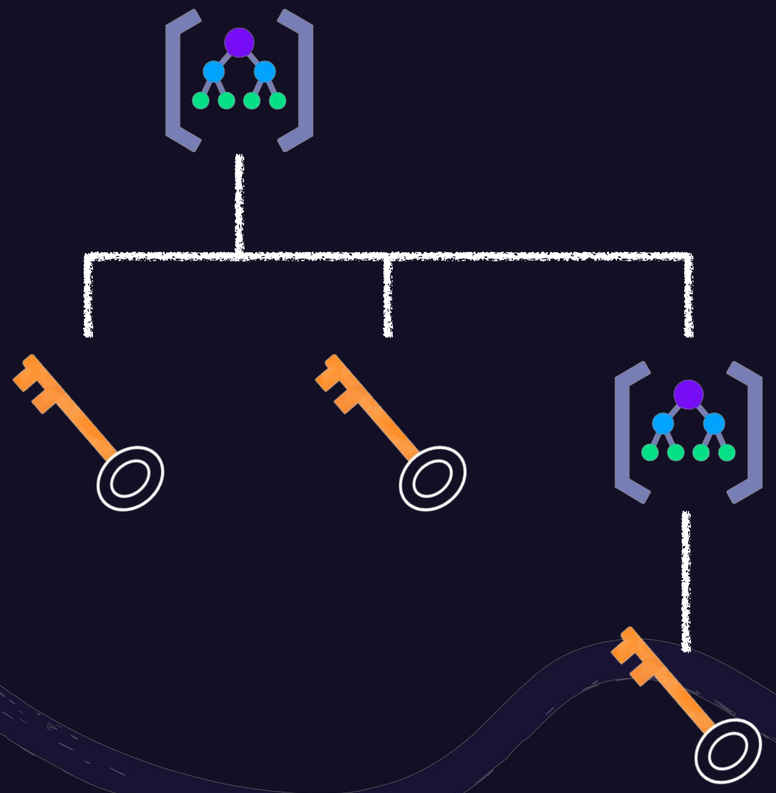
Azure Account can have multiple subscriptions



Separate subscriptions for:

- Separate billing centers
- Separate access control boundaries

Centralized management for multiple subscriptions



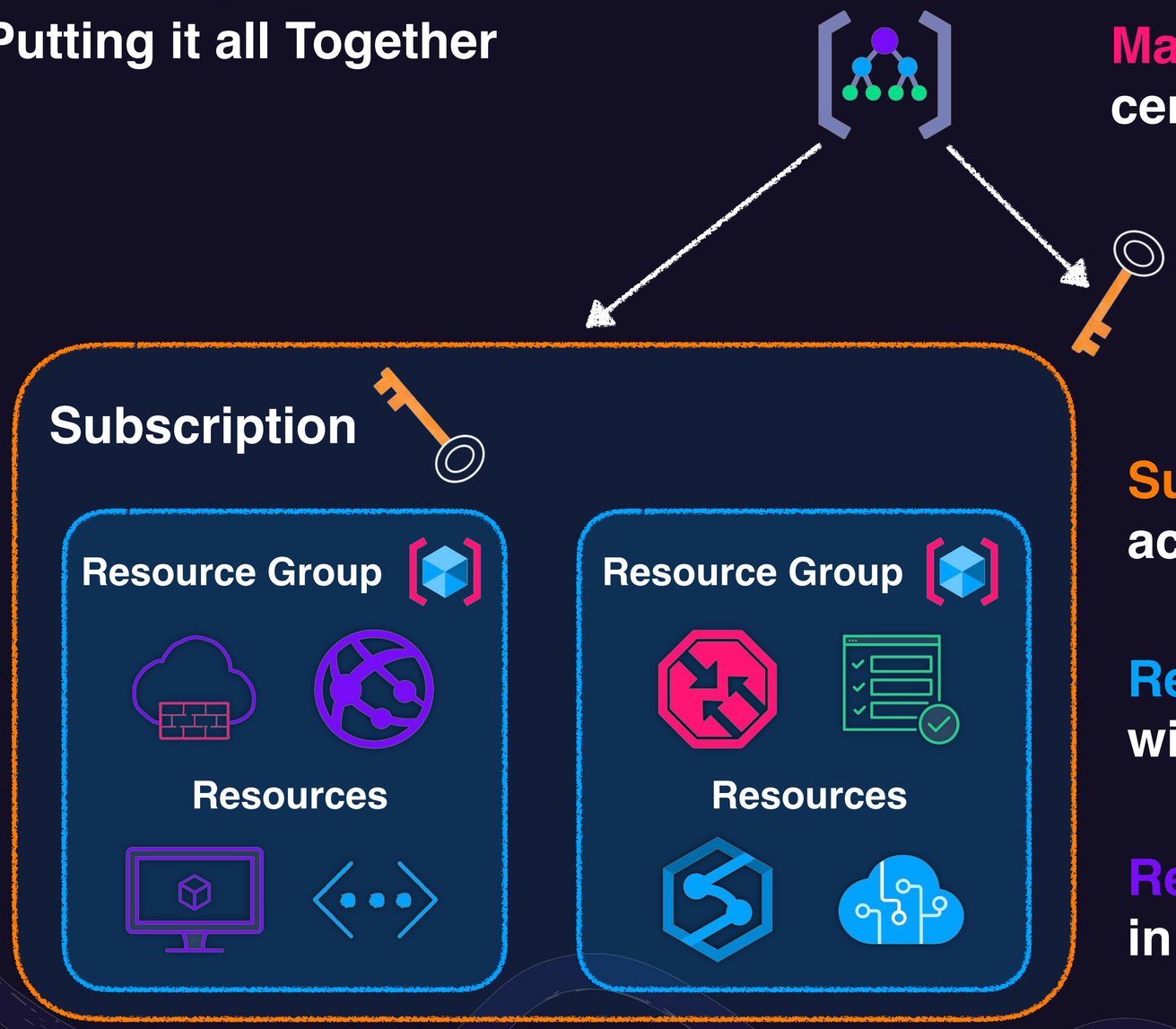
Only ‘optional’ component of resource organization

Easily manage multiple subscriptions

- Policies applied to management group applied to all child objects (more on this later)
- Ideal for larger organizations with multiple subscriptions
- Can contain child management groups

Resource Organization

Putting it all Together



Management Group = Optional centralized subscription management

Subscription = High-level billing and access control boundary

Resource Group = Groups of resources with same lifecycle/access control needs

Resources = Everything you create in Azure

Resource Hierarchy

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Resource Hierarchy

Resource Hierarchy at a Glance

Similarities to File System

Inheritance

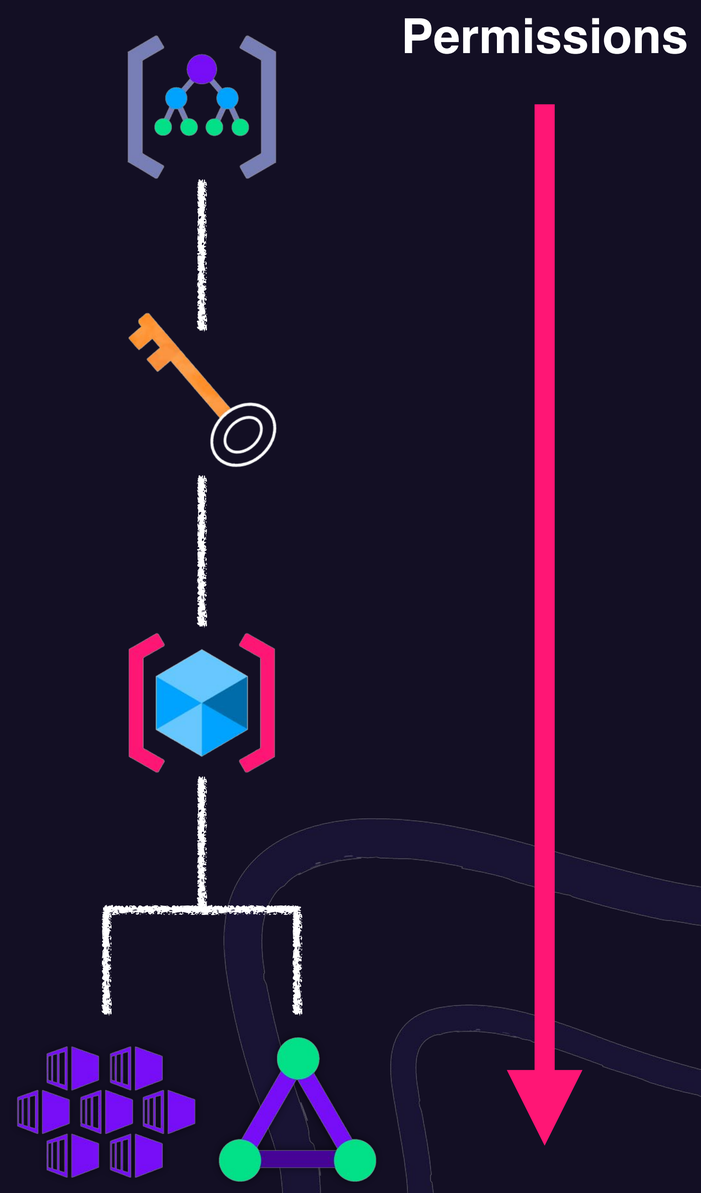
Matthew Ulasien
Azure Training Architect

Resource Hierarchy at a Glance

Policies and **permissions** are applied downward.

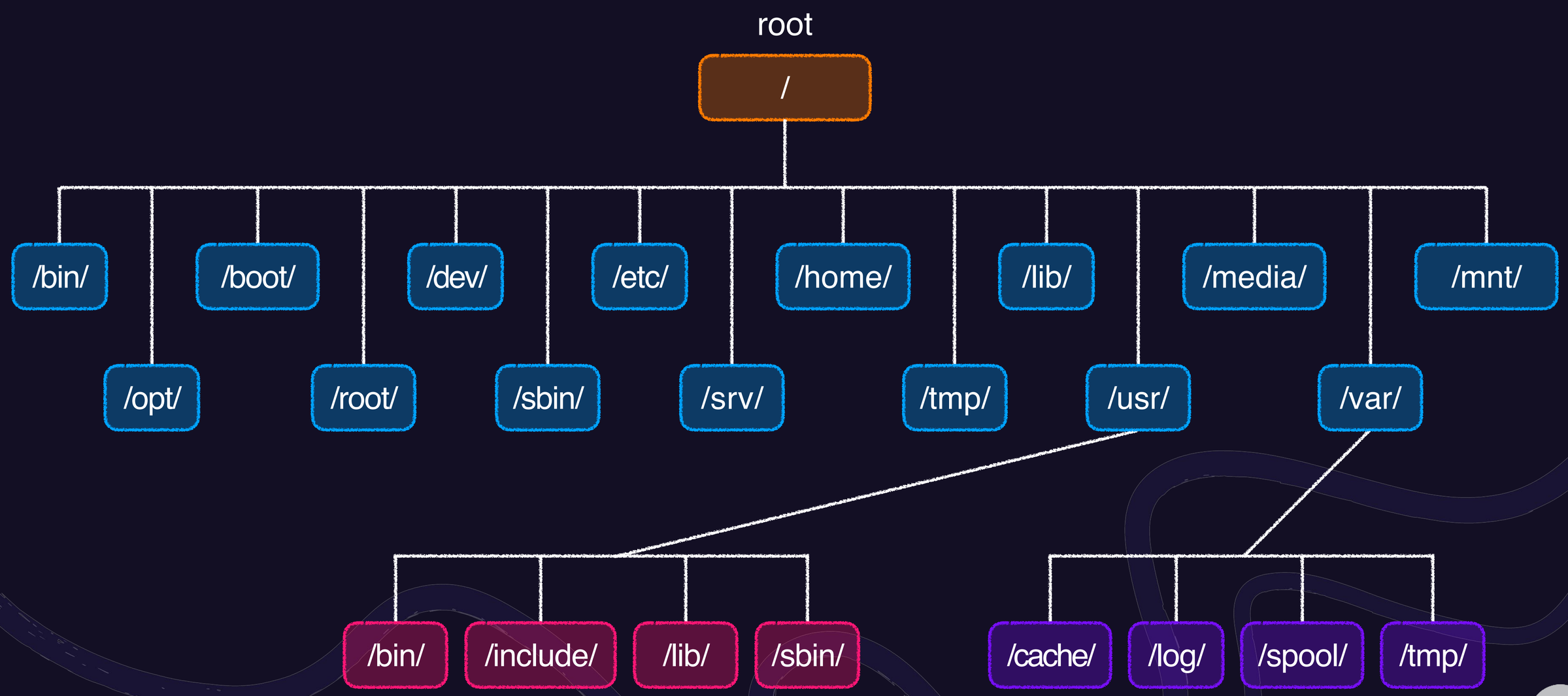
Organization and **hierarchy** is a parent-child relationship.

Goal: Unified policy access management.



Resource Hierarchy

Similarities to File System



Resource Hierarchy

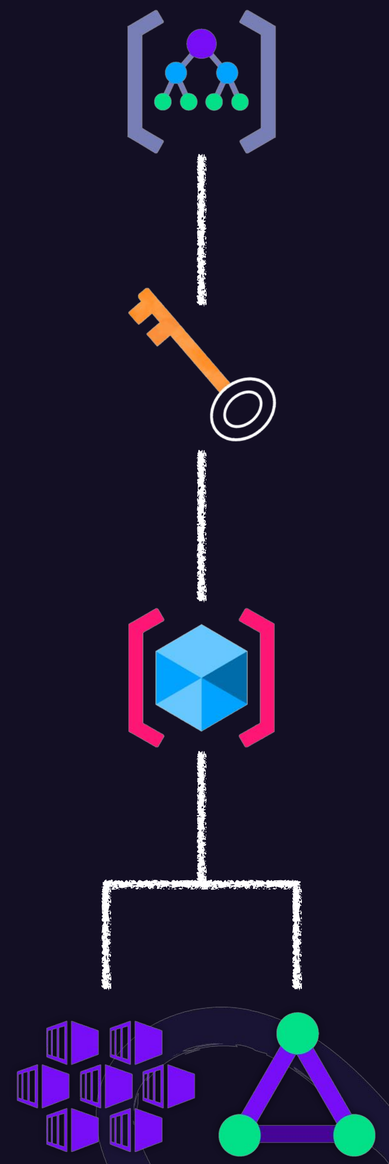
Similarities to File System

Management Group

Subscription

Resource Group

Resources

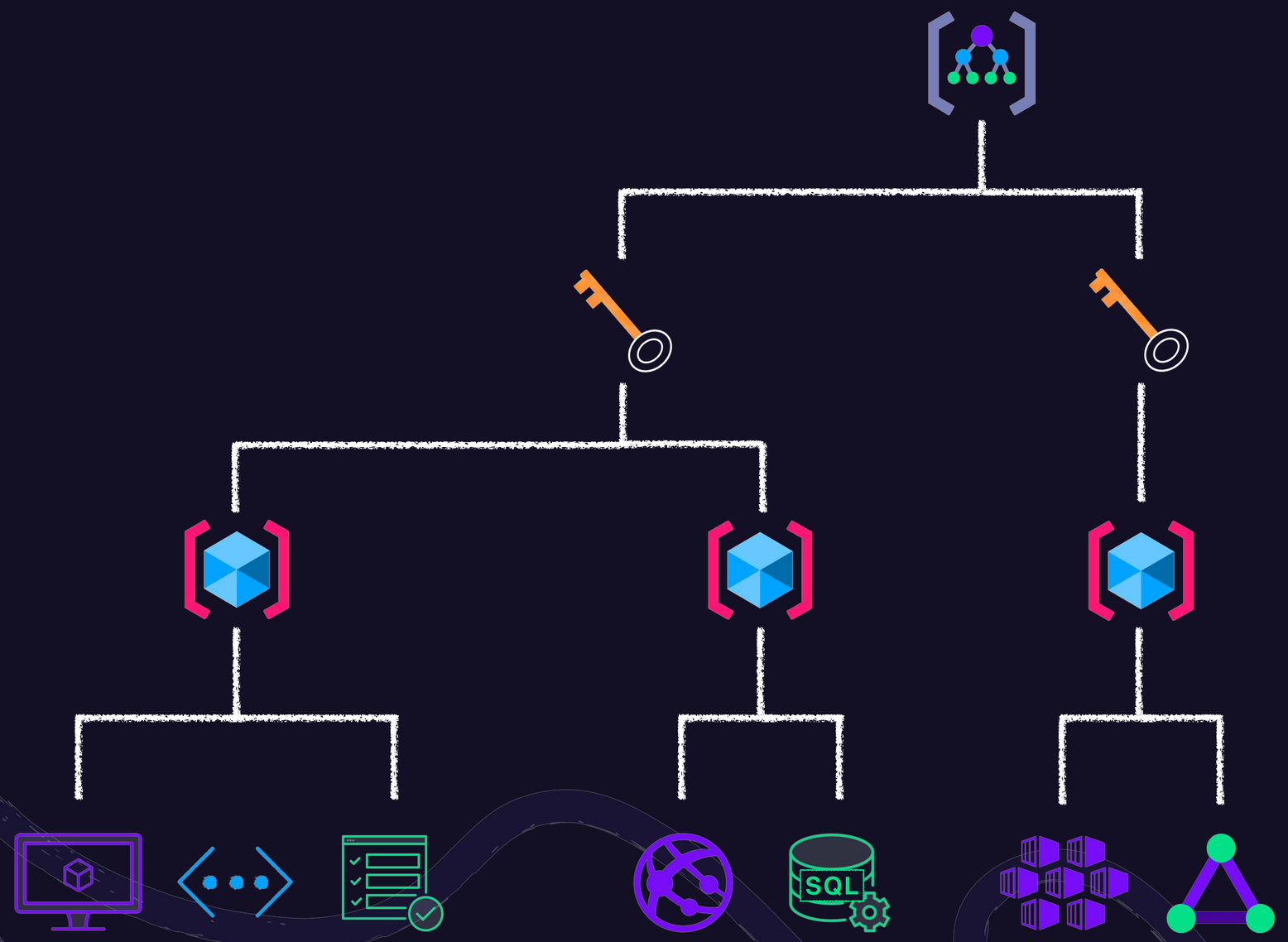


Parent

Child

Resource Hierarchy

Similarities to File System

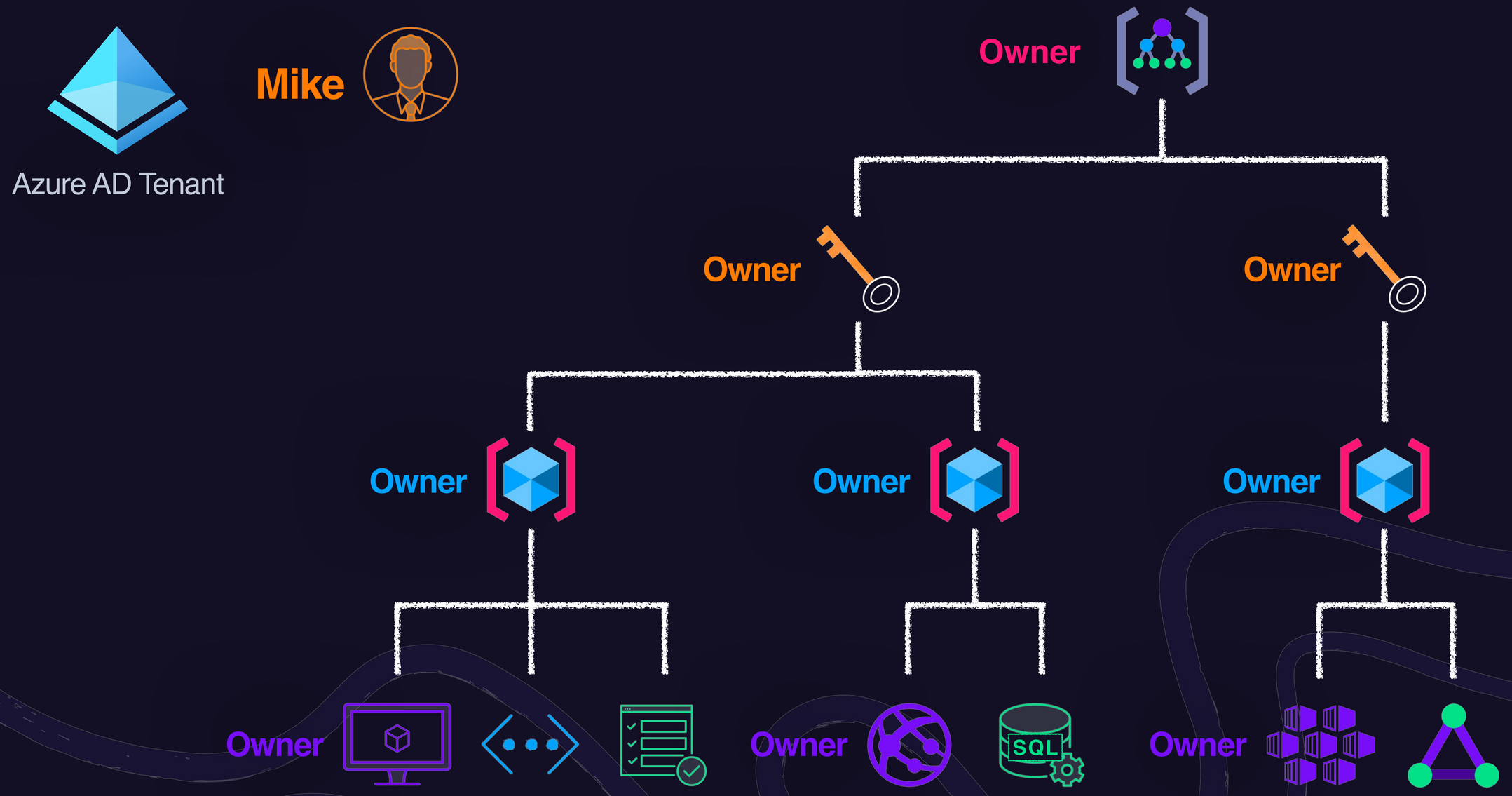


Child objects have exactly **one** parent.

Child objects **inherit** policies/ access from parent.

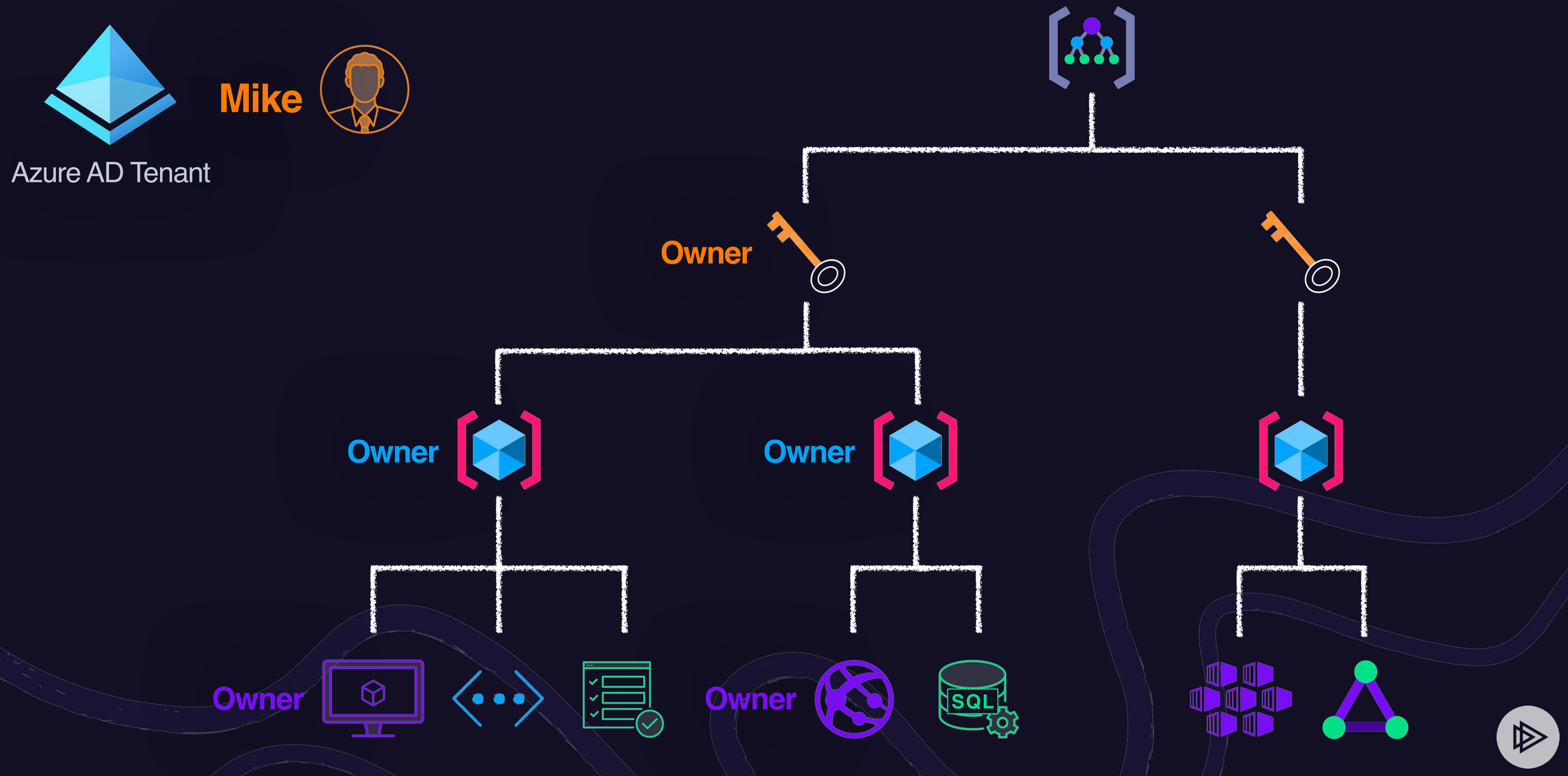
Resource Hierarchy

Inheritance



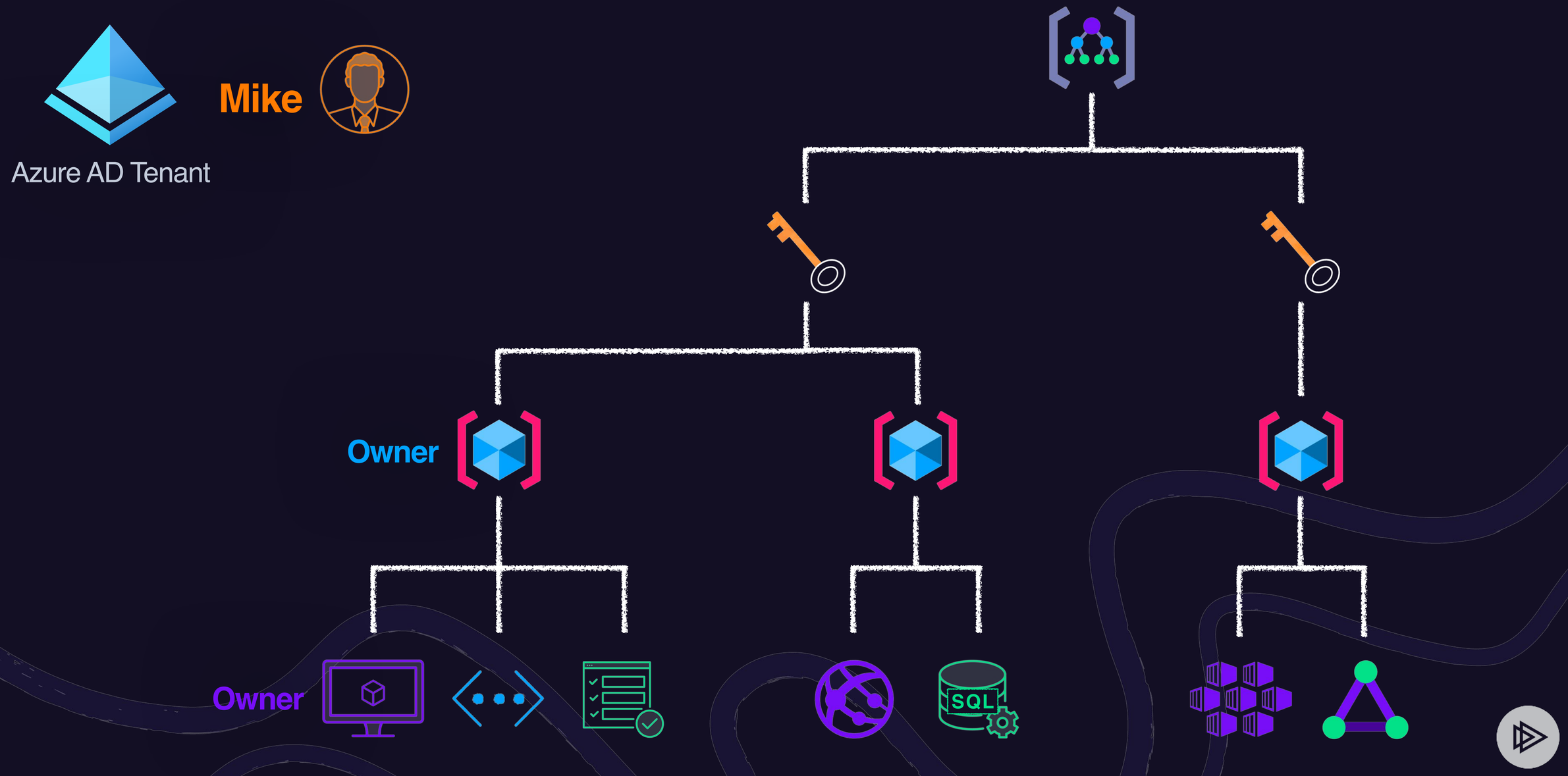
Resource Hierarchy

Inheritance



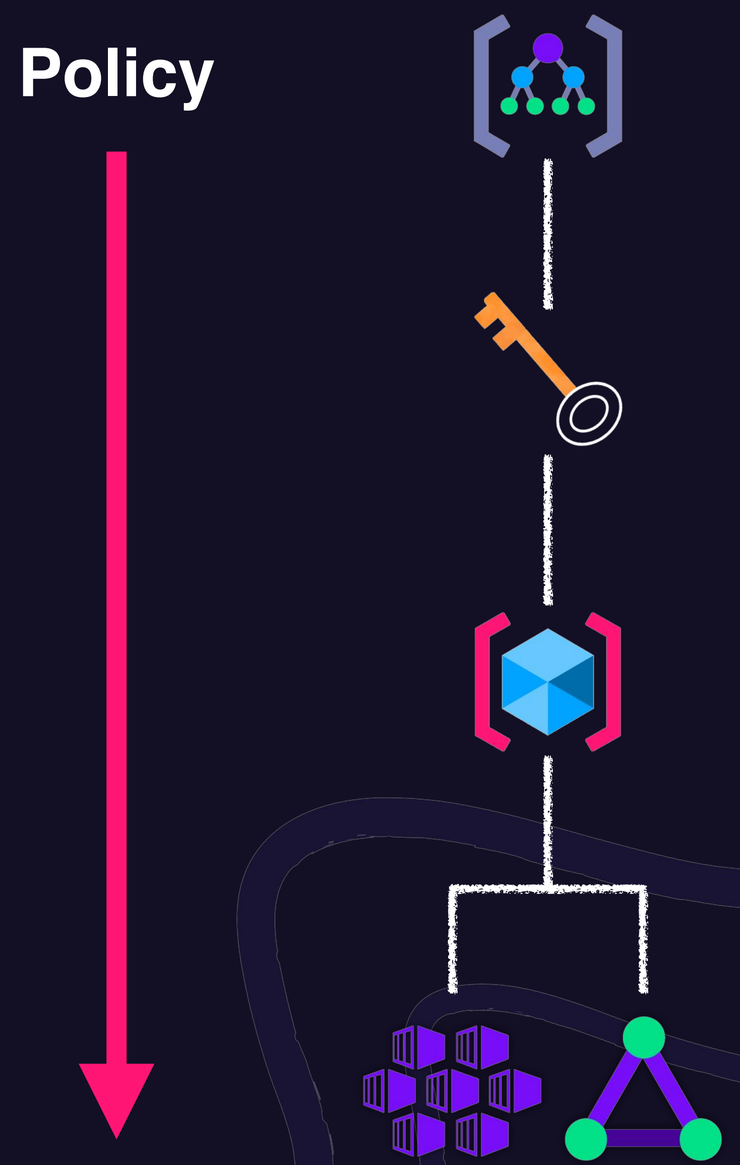
Resource Hierarchy

Inheritance



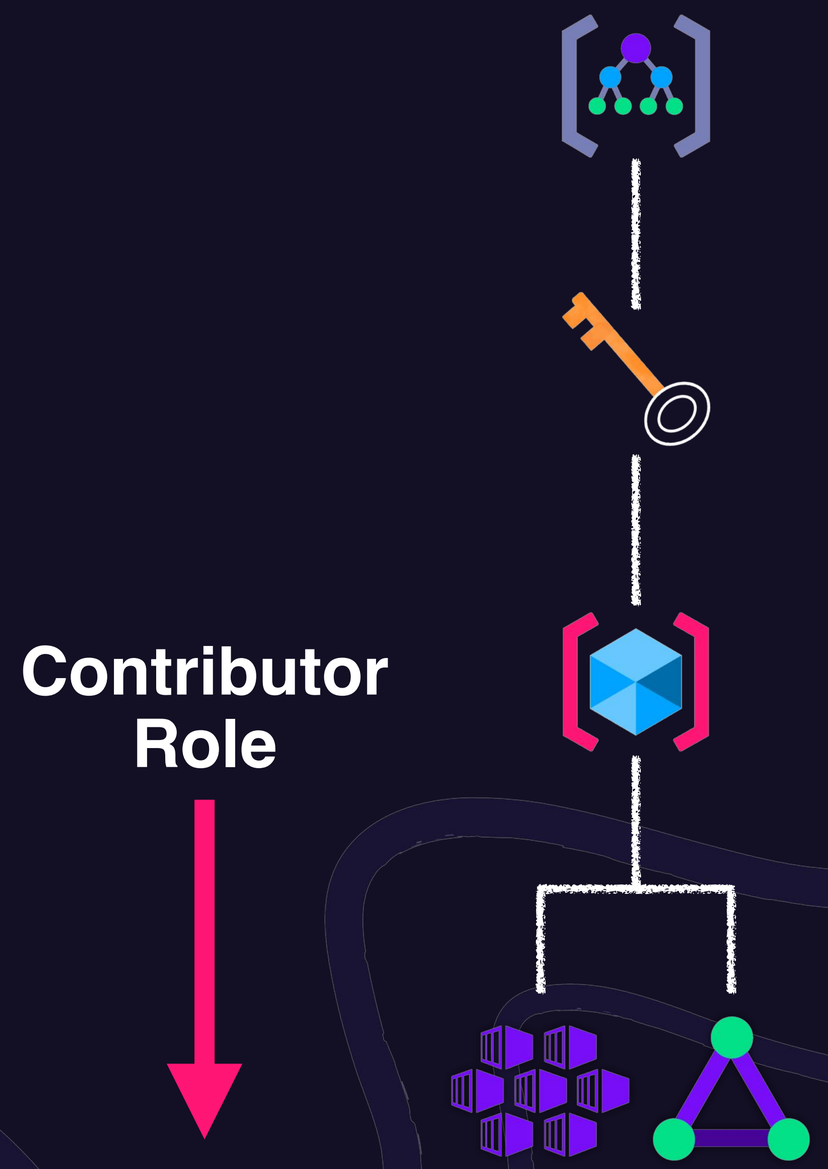
Inheritance Examples

Azure Policy: Limit VM location to US Central at management group.



Inheritance Examples

RBAC: Give Contributor role to resource group.



Summing It Up

Resource Hierarchy: The Big Idea

- Policies and permissions are applied from parent to children objects.
- Each child object can have exactly one parent object.
- Each parent can have multiple child objects.

Exam Tips: Architectural Components of Azure

Matthew Ulasien
Azure Training Architect

Azure Regions

Globally distributed groups of datacenters

Azure Regions

Each region = several nearby datacenters

- Resources are assigned to a region
- Location/features/price key factors

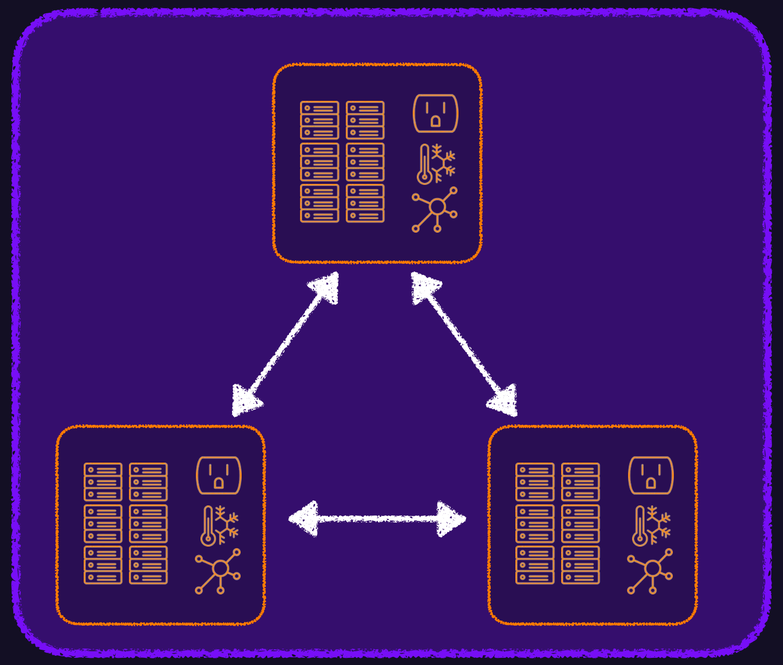
Region Pairs

- Each region paired with another one in country (except Brazil)
- Redundancy/failover location

Sovereign Regions

- Isolated regions for government compliance
- Azure for US Government
  - Government agency or contractors only
- Azure China
  - Must have to do business in China
  - Managed by third-party company

Availability Zones



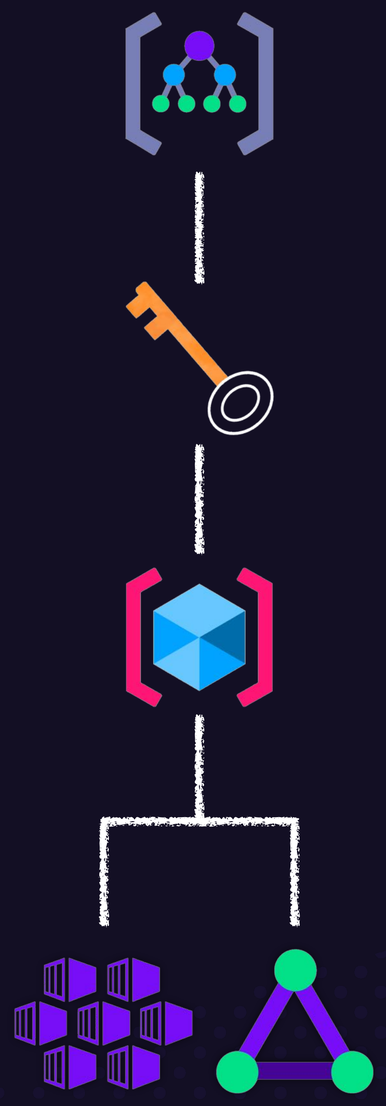
Fault Isolation <u>within region</u>

- Independent datacenters within region
- Plan to add redundancy to your application/solution
- If one fails, another in the region still works

Using Availability Zones

- Zonal: Pin resource to specific zone
- Zone-redundant: Service automatically replicates across multiple zones

Resource Organization



Understand purpose of each layer

Resources:

Everything you create on Azure

Resource Groups:

Hold resources with same access/lifecycle needs

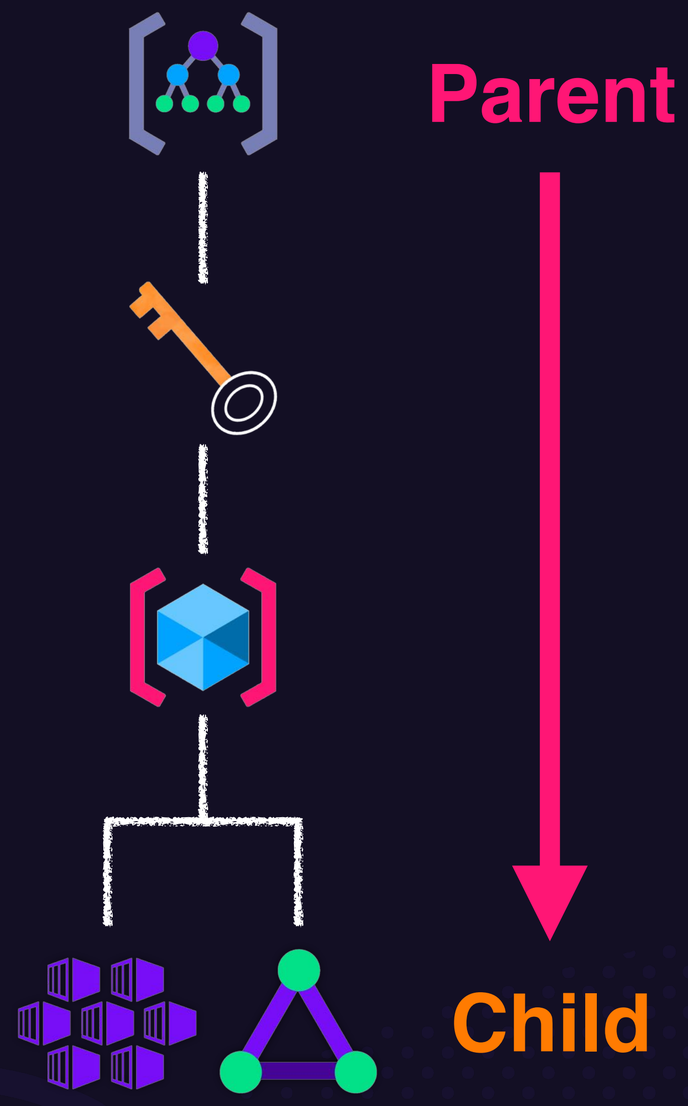
Subscriptions

- Contain multiple resource groups
- Billing and access boundary

Management Groups

- Centrally manage multiple subscriptions
- Optional component

Resource Hierarchy



Top-down application of access/ policies

Child objects have exactly **one** parent.

Child objects **inherit** access/policies from parent.

Azure Compute Concepts

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Azure Compute Concepts

Defining ‘Compute’

Azure Compute Options

Revisiting IaaS vs. PaaS

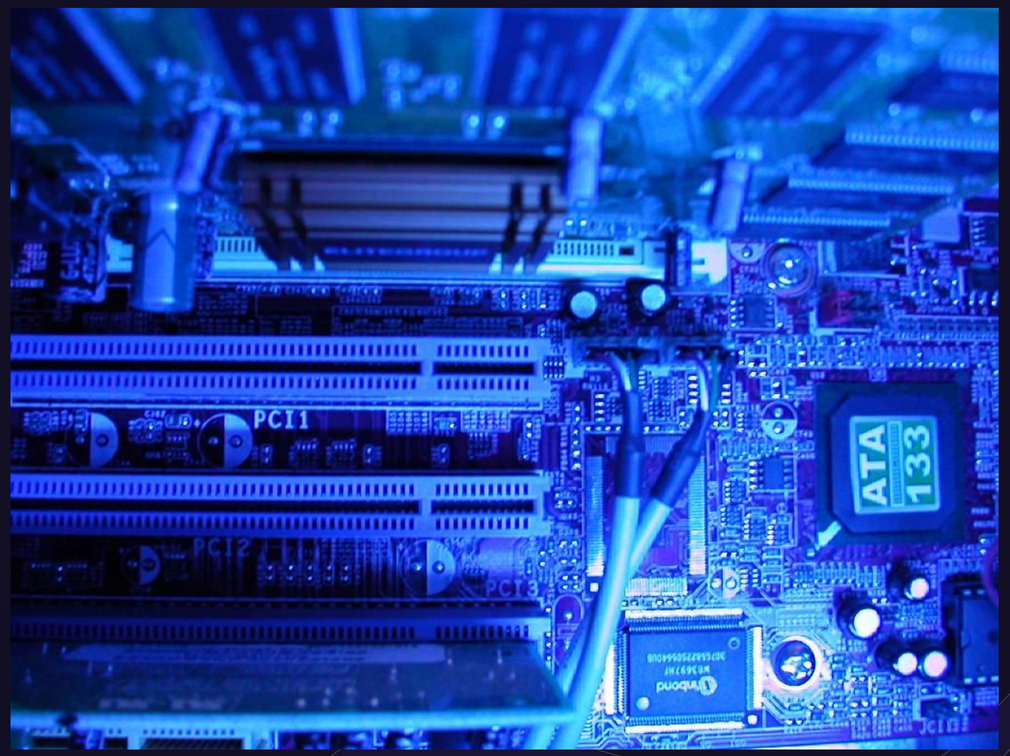
Matthew Ulasien

Azure Training Architect

Defining ‘Compute’

Azure **compute** is an on-demand computing service that provides computing resources such as disks, processors, memory, networking, and operating systems.

Definition from Microsoft documentation



“The Engine Running Your Code/Applications on Azure”

Azure Compute Options

Different Compute Options for Different Requirements

IaaS

Virtual Machines

PaaS

Azure App Service

Azure Functions

Azure Container Instances

Azure Kubernetes Service

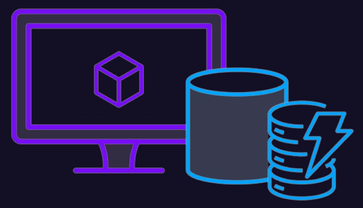
Revisiting IaaS vs. PaaS

	Responsibility	SaaS	PaaS	IaaS	On-prem
Customer is always responsible	Information and Data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and Identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and Directory Infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network Controls	Microsoft	Shared	Customer	Customer
	Operating System	Microsoft	Microsoft	Customer	Customer
Cloud provider is responsible	Physical Hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical Network	Microsoft	Microsoft	Microsoft	Customer
	Physical Datacenter	Microsoft	Microsoft	Microsoft	Customer

Microsoft Customer Shared

Revisiting IaaS vs. PaaS

Trade-offs of Flexibility vs. Management Overhead



IaaS

- Greater customization/control
- More management overhead

PaaS

- Less customization/control
- Less management overhead

Virtual Machines

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Virtual Machines

- What Is a Virtual Machine (VM)
- Behind the Scenes (Review)
- VM Components
- VMs and Networking
- Description of VM Sizes
- VM Pricing
- Use Cases for VMs

Matthew Ulasien
Azure Training Architect

What Is a Virtual Machine (VM)

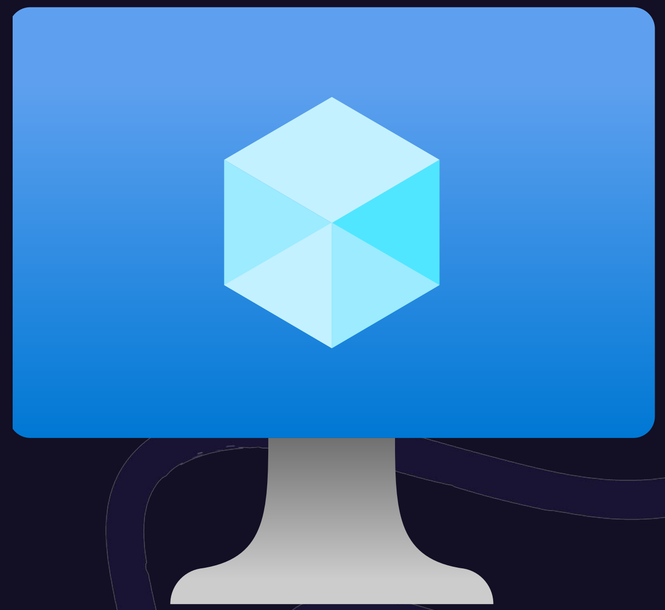
Customizable, Scalable, and On-Demand Server

Infrastructure as a Service (IaaS)

Virtualized server

- Hosted on underlying hypervisor
- You have full control over the virtualized server
- Run almost any application

Windows or Linux Operating Systems



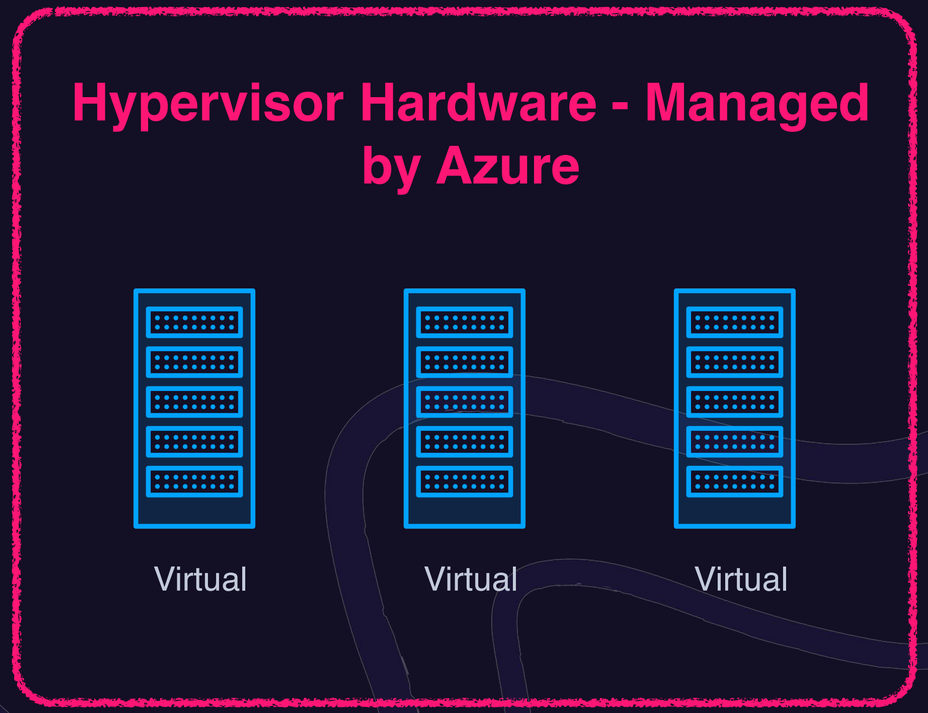
Behind the Scenes (Review)

Single Physical Server (Hypervisor) Hosting Multiple/Individual VMs

Hypervisor software hosts VMs.

You manage a single VM that is only for you.

VMs are completely isolated from each other.

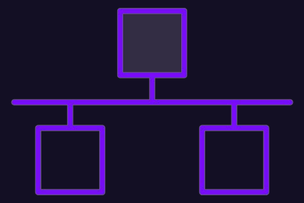


VM Components

VMs Have All the Same Required Components of a Physical Computer

CPU/Memory

Disk



Networking

Operating System (OS)

Network Controls (Firewall)

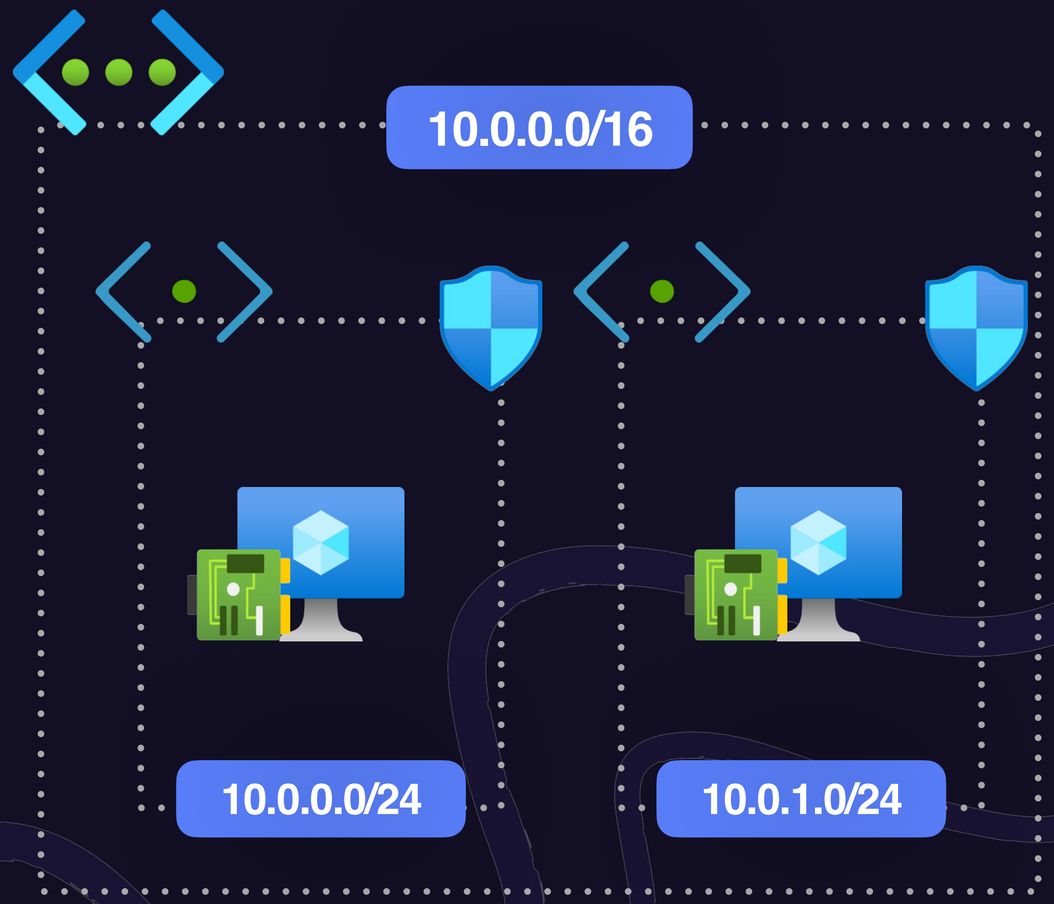
VMs Must Be Deployed to a Network

Virtual Network (VNet)

- Includes one or more subnets

VM assigned private and public IP address(es)

- Private required, public optional
- Attached to Network Interface Card (NIC)



Choose CPU, RAM, and Disk Configurations

VM Size = Preconfigured CPU/RAM combinations

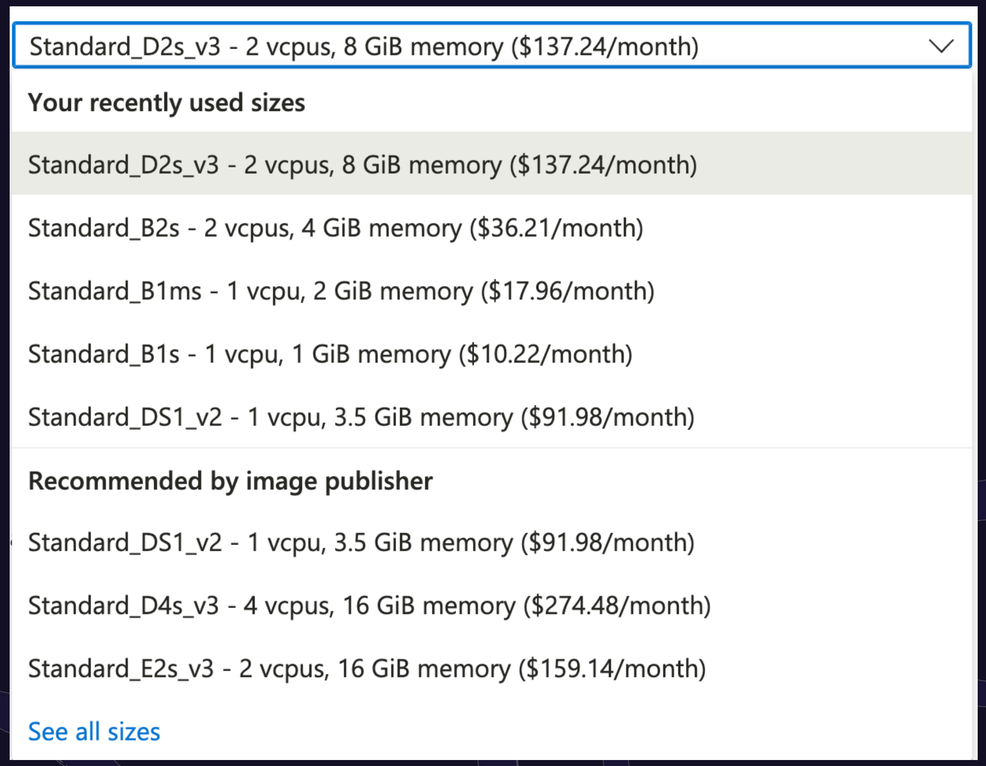
- Optionally, GPU and Disk types

VM Sizes grouped into series

- Examples: A series, B series, D series
- Different series for different use cases

Configure Disk(s)

- Various sizes/speeds

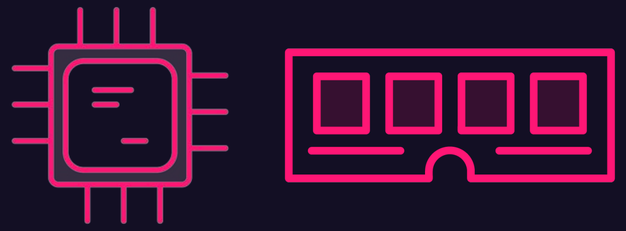


Description of VM Sizes

Type	Sizes	Description
General purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5, DCasv5, DCadsv5	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	F, Fs, Fsv2, FX	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, Easv4, Eav4, Epdsv5, Epsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2, ECasv5, ECadsv5	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	Lsv2, Lsv3, Lasv3	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NC, NCv2, NCv3, NCasT4_v3, NC A100 v4, ND, NDv2, NGads V620, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High performance compute	HB, HBv2, HBv3, HBv4, HC, HX	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

Different Pricing For Different Components

CPU/RAM (Compute)



- Priced by the minute
- More compute = higher costs
- Deallocated (stopped) VMs not charged for compute

Disk(s)

- Charged whether VM is running or not

VM Pricing (continued)

Licensed OSs

- Windows, Red Hat, etc
- Pay-as-you-go license charged same as Compute

Public IP Address(es)

- Charged by the hour
- Pricing model depends on SKU

  Dynamic: No charge when VM deallocated

  Static: Charged regardless of VM state
- More on this later

Use Cases for VMs

Pros and Cons

Pros:

+

Control

Use virtual machines when you need to control all aspects of an environment or machine.

+

Application Compatibility

Install specific applications on your Windows or Linux machines.

Better legacy support.

+

Existing Infrastructure

You can move existing resources and virtual machines to Azure from on-premises or another cloud provider.

“Lift and shift”

+

Testing and Development

Quickly and easily test applications and configurations.

When done, simply delete the VM.

+

Extend Your Datacenter

Extend your on-premises servers to work with Azure VMs.

Hybrid cloud.

Useful for disaster recovery.

Use Cases for VMs

Cons:

More ‘stuff’ to manage

Much more management overhead.

OS updates, patches, user control, software environments, database configurations, etc.

Higher costs

Specialized services for cloud-native applications often cost less.

Complexity in Scaling

Scaling is often a more manual process.

Scale sets help, but still not as automated as PaaS services.

Summing It Up

What Is a Virtual Machine?

- On-demand server
- Infrastructure as a Service (IaaS)

VM Pricing

- Compute/LIcensed OS: Only when running
- Disk: Always charged regardless of state
- IP address: Depends on SKU

Use Cases (Pros and Cons)

- Full control
- Run any software
- Extend your datacenter
- Much more to manage

Demo: Creating Virtual Machines

Matthew Ulasien
Azure Training Architect

Demo

Create two virtual machines

- Windows and Linux

Pay attention to:

- Resource organization
- Required region to assign
- Options with OS, VM size, and networking
- Open ports for connected access (next lesson)

Summing It Up

Creating a Virtual Machine

- Must assign to:
  - Region
  - Resource group
  - Network

Many Configuration Options

- VM size
- Operating system
- Disks
- And much more!

Demo: Connecting to Virtual Machines

Matthew Ulasien
Azure Training Architect

Demo

Connect to Windows and Linux VM from previous lesson.

- Windows: RDP port 3389
- Linux: SSH port 22

Delete VMs and associated components when finished.

Summing It Up

Connecting to Virtual Machines

- Different processes for Windows and Linux
  - Windows: Remote Desktop over TCP:3389
  - Linux: SSH over TCP:22
- Lock down ports in production environment

Virtual Machine Scale Sets

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

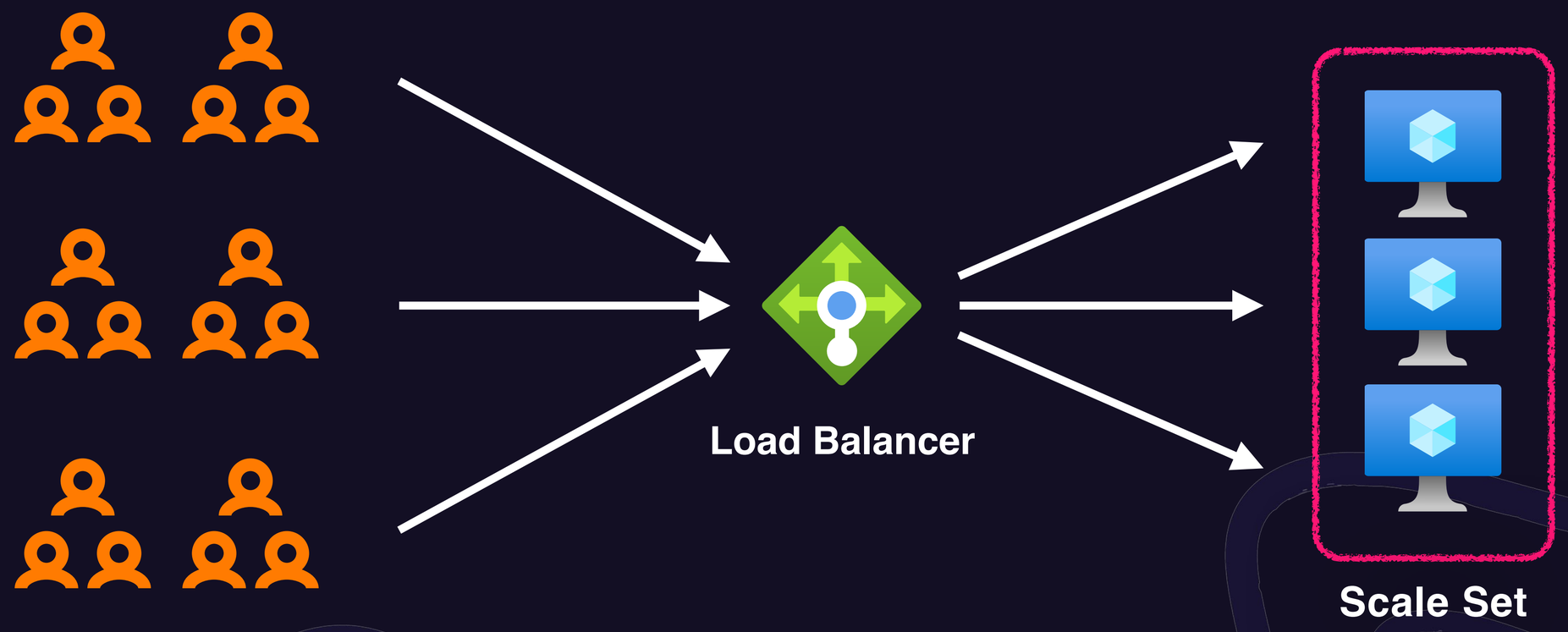
Virtual Machine Scale Sets

- What Are Virtual Machine Scale Sets (VM)?
- Problem to Solve
- How VM Scale Sets Work
- Benefits
- Creating Cloned VMs

Matthew Ulasien
Azure Training Architect

What Are Virtual Machine Scale Sets (VM)?

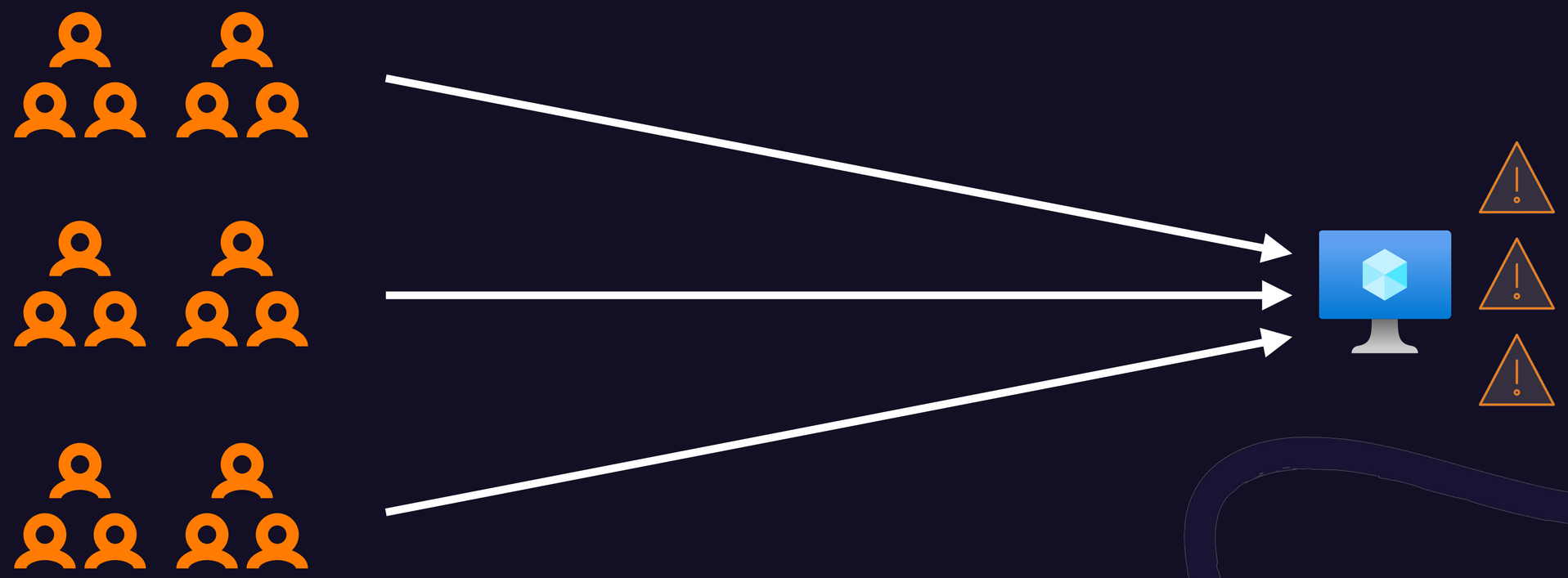
Auto-scaling Groups of Identical VMs



Create and manage multiple, load-balanced, and identical VMs.

Problem to Solve

Too Much Load/Traffic for Server to Handle



Manually creating new VMs is a time-intensive process.

Need to <u>automatically</u> create <u>copies</u> when needed.

How VM Scale Sets Work

Multiple identical VMs

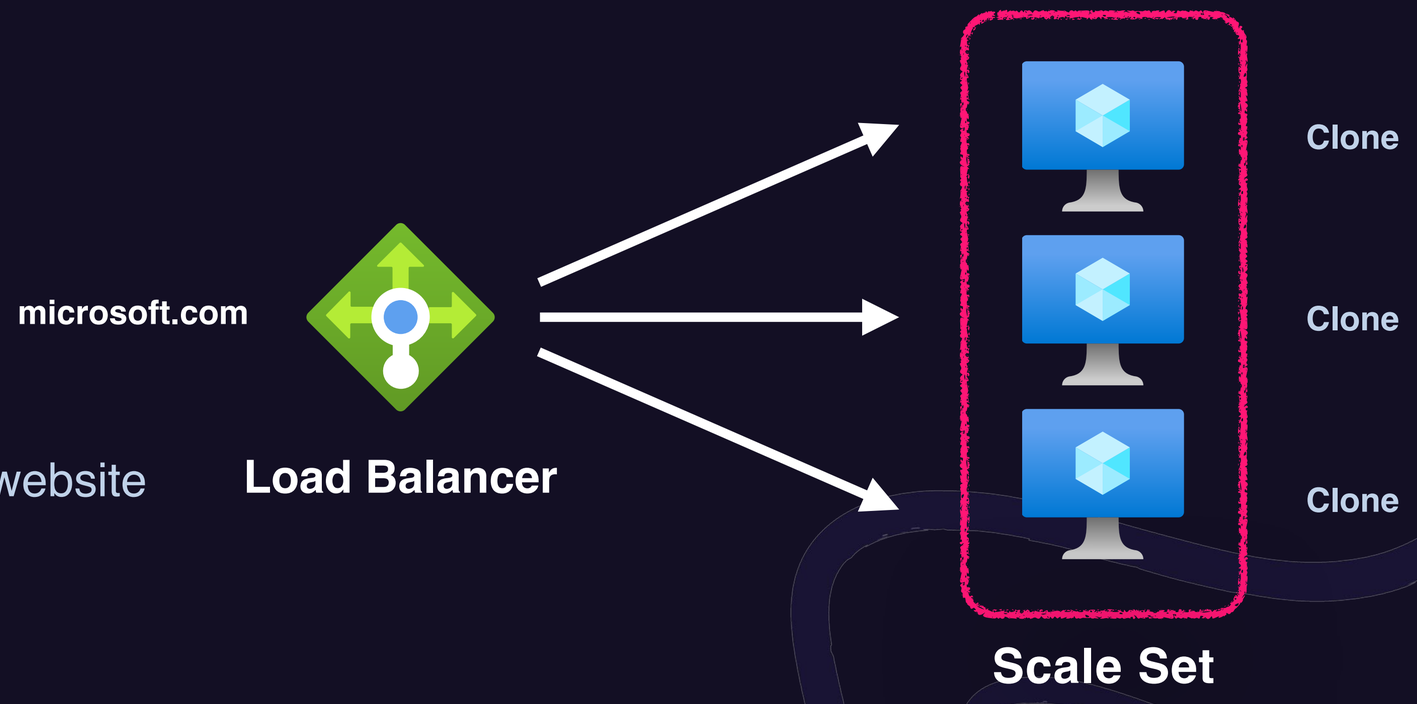
- Identically configured
- All managed from the same place

Behind a Load Balancer

- Directs traffic to available VMs
- Single frontend for users (e.g., a single website address)

Increase/decrease VM count

- Can automatically or manually adjust count
- Horizontal scaling



Benefits

Multiple VMs

Simple to manage multiple identical VMs using a load balancer.

High Availability

If one VM fails or stops, the others in the scale set will keep working.

VMs can be deployed across multiple zones in single region

Zone-redundant

Auto Scaling

Automatically match demand by adding or removing VMs from the scale set.

Large Scale

Run up to 1000 VMs in a single scale set.

No Extra Cost

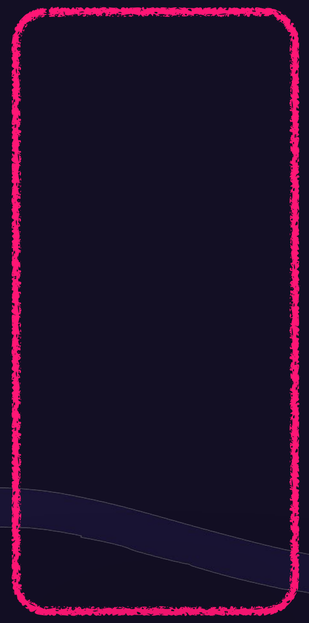
No added cost for using scale sets.

Creating Cloned VMs

From baseline image

- Capture image from baseline/reference VM
- Scale Set VMs created from captured image

Baseline Image



Scale Set

Creating Cloned VMs

From baseline image

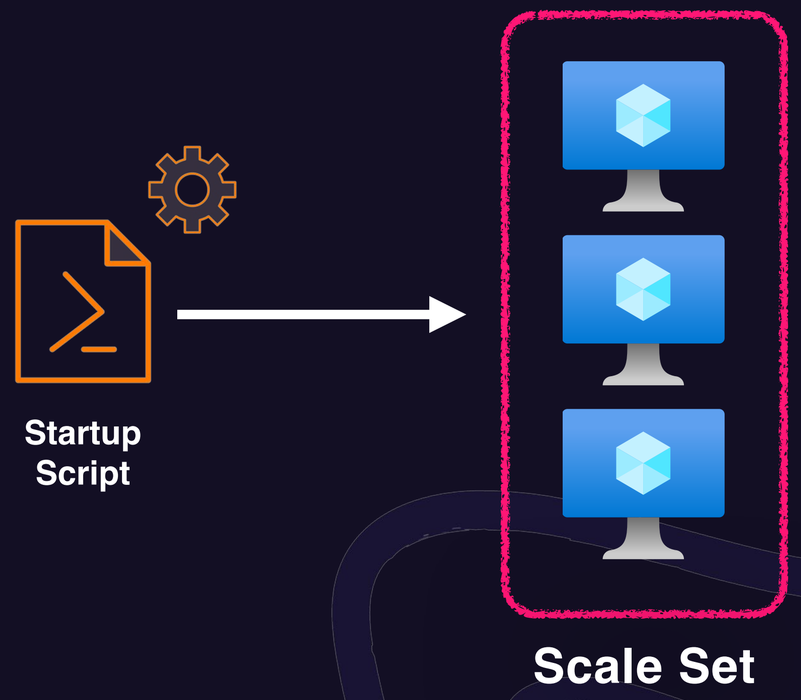
- Capture image from reference VM
- Scale Set VMs created from captured image

Configuration script at startup

- New clone VM runs configuration script on first boot

Combination of both

- Reference image + additional configurations



Summing It Up

Scale Sets = Identical VMs

- Create and remove as needed
- Centrally managed

Purpose

- Handle increased/decreased load as usage grows/shrinks
- Automatically or manually adjust count
- Paired with load balancer

Creating Clones

- Baseline image
- Configuration script

Availability Sets

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Availability Sets

Purpose of Availability Sets

Breaking Down Availability Sets

When to use Availability Sets?

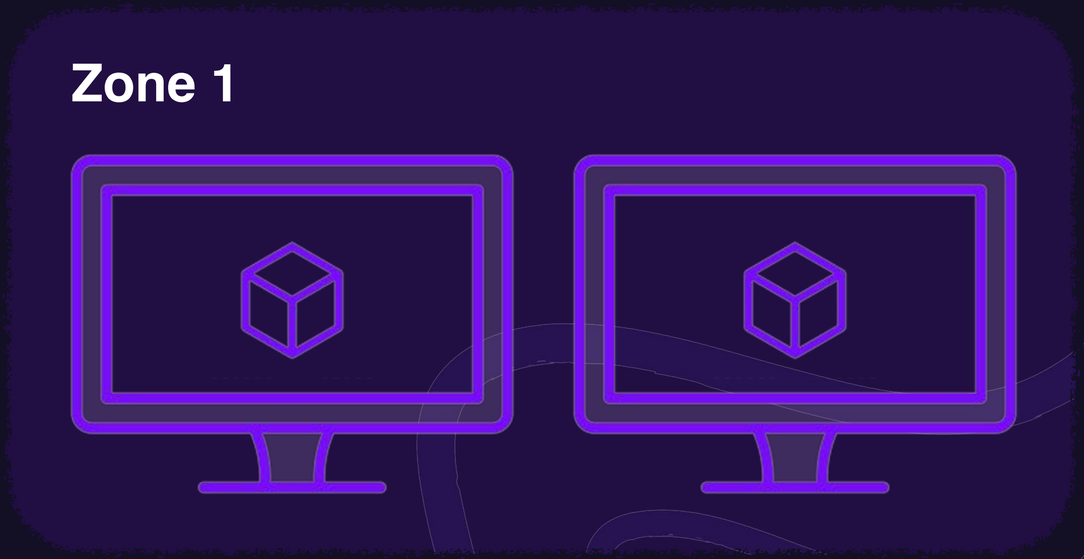
Matthew Ulasien
Azure Training Architect

Purpose of Availability Sets

High Availability for Static VMs in Single Datacenter/Zone

Differences compared to Scale Sets:

- Non-identical VMs
- No auto-scaling
- Single datacenter/zone

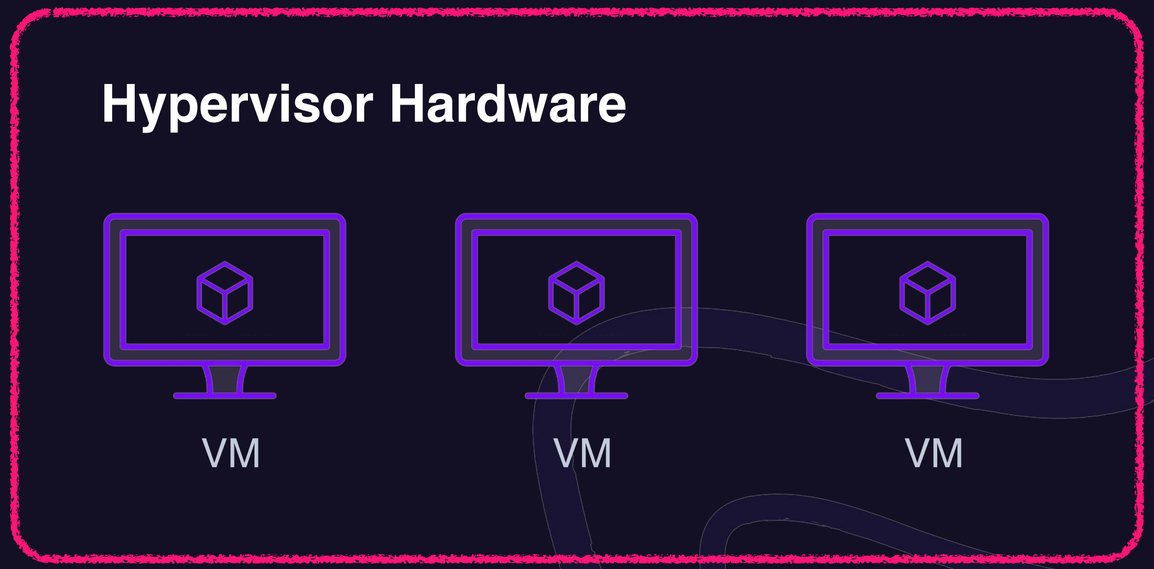


Breaking Down Availability Sets

Logical Grouping of VMs with Separate Fault and Update Domains for High Availability

What are fault and update domains?

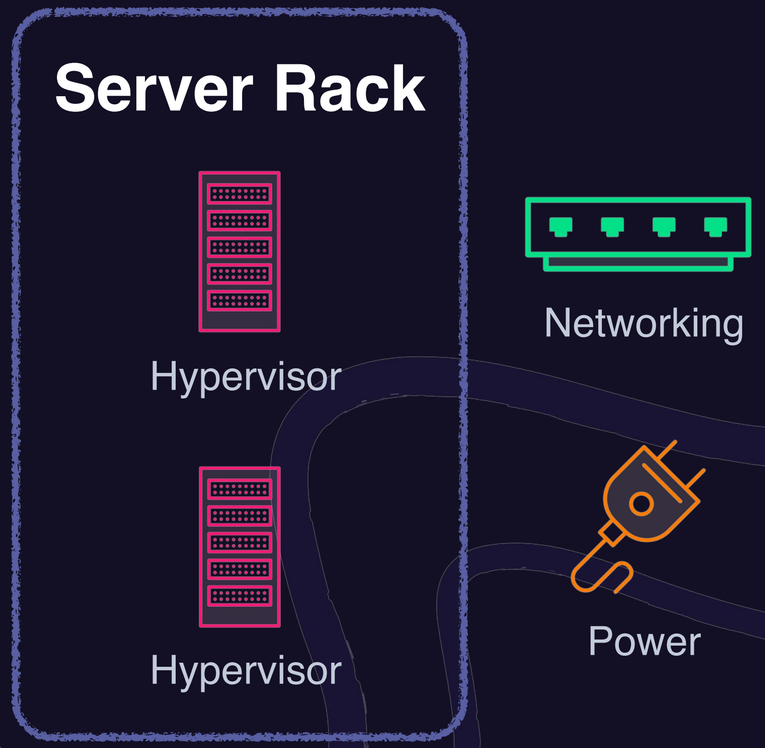
Let's talk about the underlying hypervisor hardware.



Hypervisors with Common Power Source/Network Switch

Example: Hypervisors on same server rack

VMs on hypervisors with same power/ networking = single fault domain



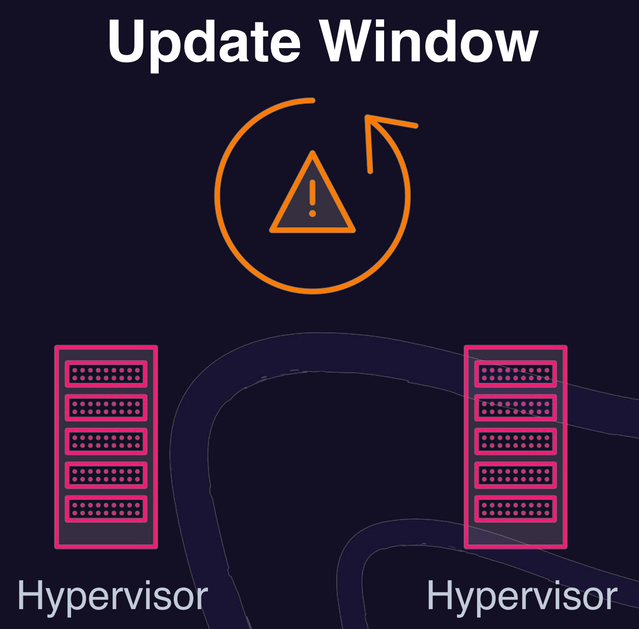
Update Domain

Groups of Hypervisors (and VMs) That Can Be Rebooted at Same Time

Planned hypervisor maintenance updates

Not dependent on physical rack/location

Two VMs in same update domain may both be temporarily unavailable at same time



Spreading VMs across Update/Fault Domains

Adding static VMs to an availability set ensures VMs are placed:

- On hypervisors with separate maintenance windows
- On hypervisors on different server racks
- Result: High availability in case of power supply failure and/or rolling hypervisor updates

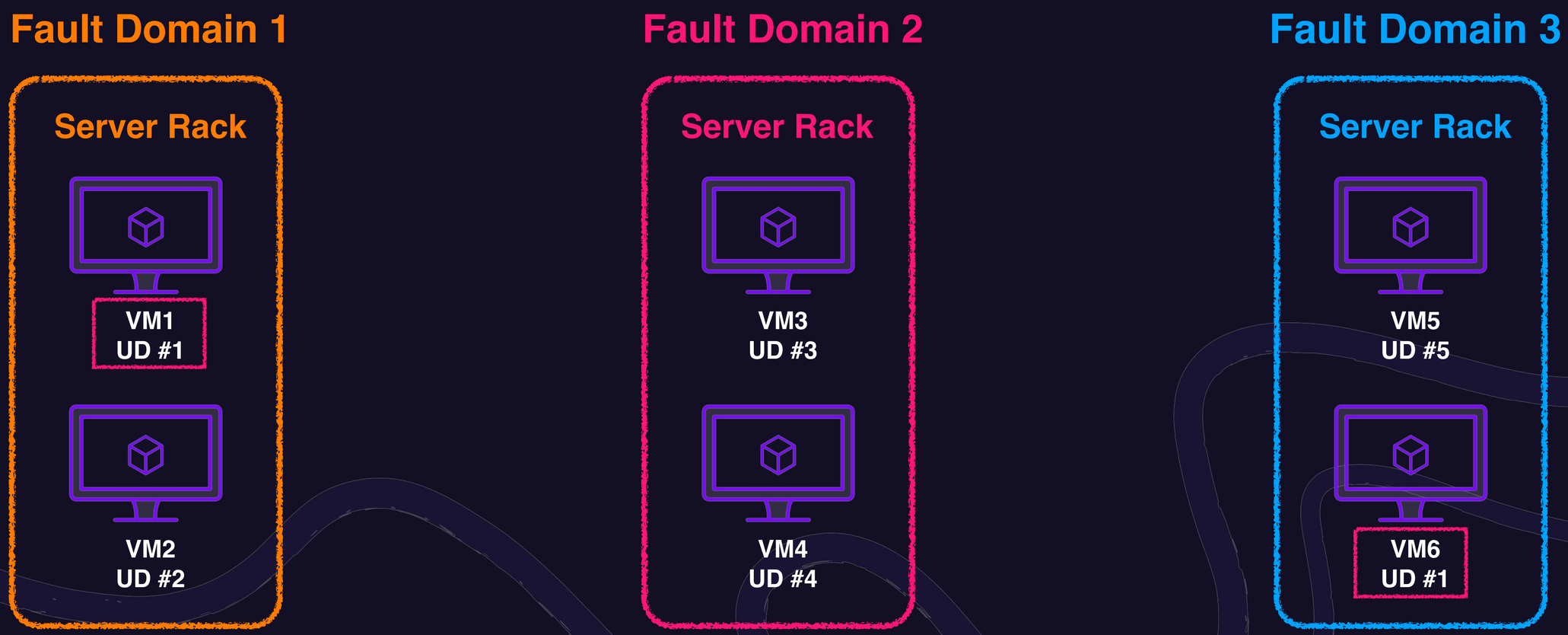
Visual Example

Example Availability Set Configuration:

- 5 Update Domains
- 3 Fault Domains

Max Limits:

- 20 Update Domains
- 3 Fault Domains



When to Use Availability Sets?

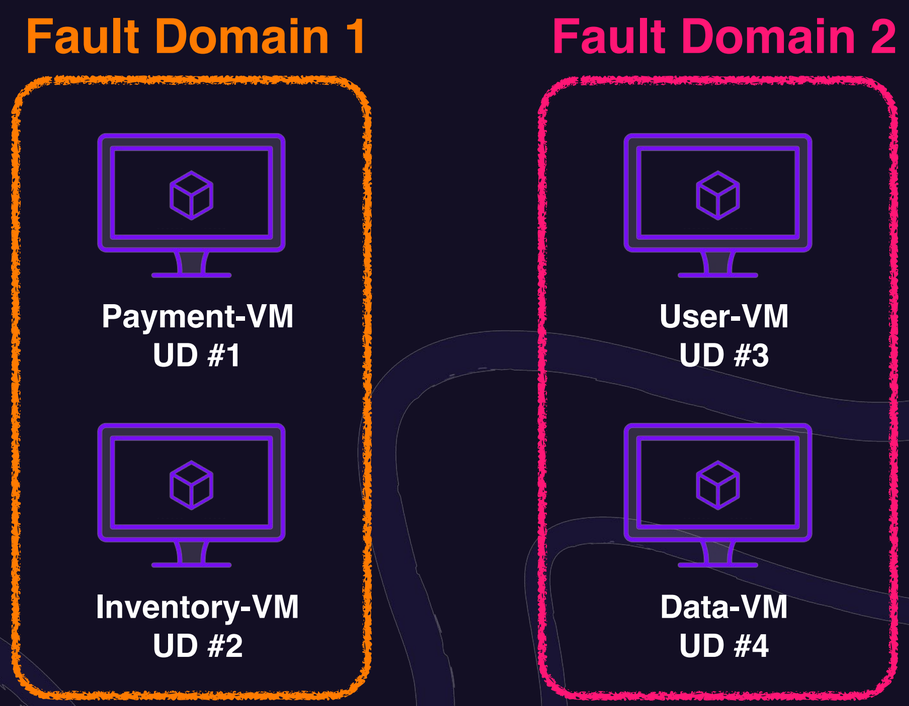
High Availability for Multiple Unique VMs That Don’t Need Auto-Scaling

Example: E-commerce site with multiple servers

- Payment processing
- Inventory management
- User authentication
- Data analytics

VMs can’t easily be cloned

No auto-scaling needed



Summing It Up

What Are Availability Sets?

- High availability within a single zone/datacenter
- Non-identical VMs

Fault Domain

- Server rack with shared power/networking

Update Domain

- Hypervisor groups on same maintenance schedule

Azure Virtual Desktop

Matthew Ulasien
Azure Training Architect

LESSON BREAKDOWN

Azure Virtual Desktop

- Simple Definition
- Problem to Solve
- How AVD Works
- Use Cases

Matthew Ulasien
Azure Training Architect

Simple Definition

Virtualized Windows Desktops and Apps, Hosted on Azure

- Virtual Desktop Interface (VDI), powered by IaaS
- Access from **any device**
- **Separates OS**, **data**, and **apps** from local hardware
- **Centrally managed** and **secured**

How to Securely Enable a Remote Workforce?

Challenges

1. **Data Security**
   Secure data accessed from many locations

2. **IT Overhead**
   Manage multiple user desktops can be a nightmare

3. **Software Consistency**
   Making sure all users have consistent software and updates

4. **Scalability**
   Support growing workforce

How Azure Virtual Desktop (AVD) Helps

Security

- All data centrally stored in Azure
- Includes desktop and apps

Instantly Scale with VMs

- Easily add more VMs to host pool
- Multi-session environments

Central Management

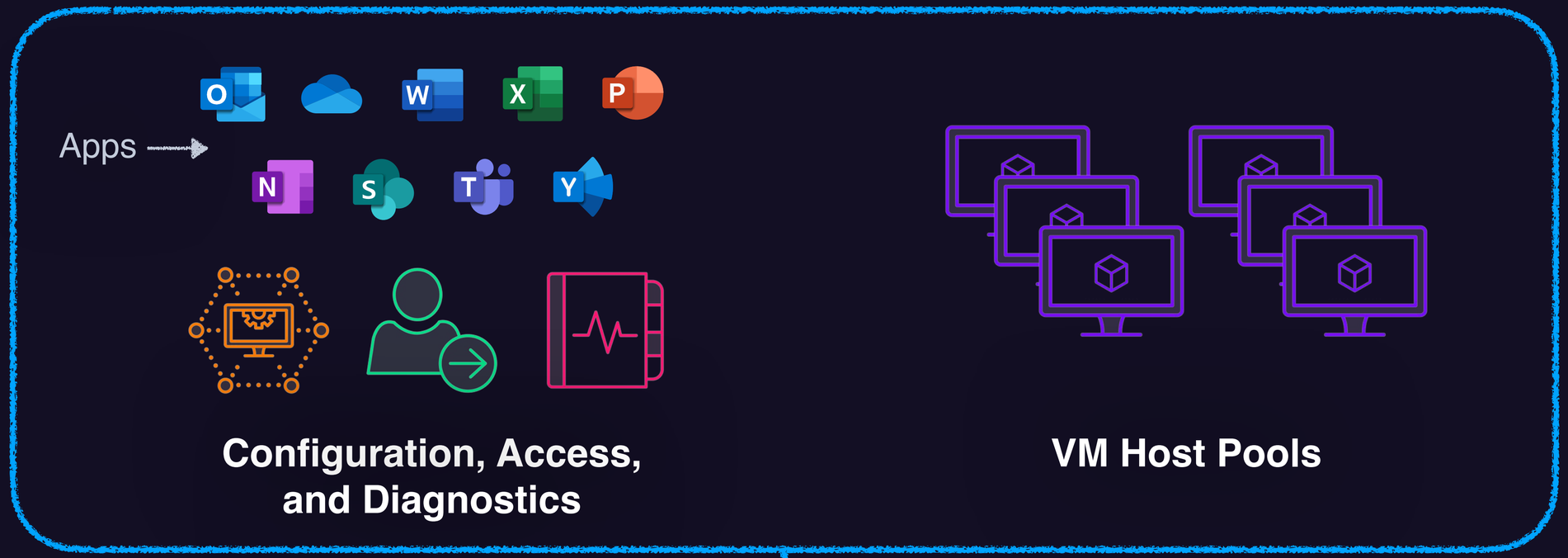
- Apps, updates, and settings centrally managed
- Use existing Windows 10/11 licenses

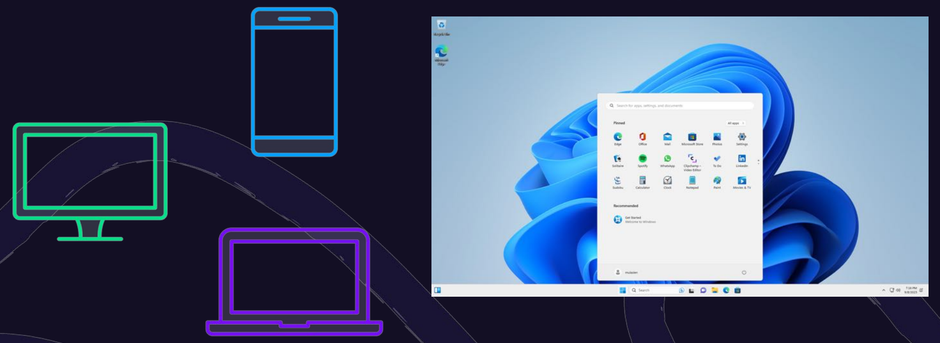
Access from any Device

- Windows, Mac, mobile devices, and web browser

Azure Virtual Desktop

How AVD Works





Use Cases

Remote Workforce Enablement

- Remote work enabled via Windows desktops from anywhere
- No need for company hardware; BYOD (Bring Your Own Device) friendly

Secure Data Handling for Healthcare

- Secure, controlled access to sensitive patient data
- Reduced risk of data breaches
- Simplifies healthcare compliance

Summing It Up

What Is Azure Virtual Desktop?

- Virtual Desktop environment (similar to Citrix)
- Access Windows apps from anywhere, but centrally managed and secured

Use Cases

- Mobile workforce
- Data security for sensitive fields

App Services

Matthew Ulasien
Azure Training Architect

What Is Azure App Service?

Fully Managed Application Hosting with Minimal Management Overhead

You bring your code, and Azure handles the rest.

No managing infrastructure (VMs)!

App Services

Things You DON’T Have to Manage

Operating system

- Configuration
- Updates

Scaling (scale sets)

- OS images
- Configuration scripts

Web server applications

- NGINX, Apache, IIS

Load balancers

Network management

Disk management

High availability

App Services

Focus on What Matters

Business Value

Your Code

Your Focus

Microsoft Manages

Servers

Network

Storage

App Service Hosting Capabilities

Web Apps

- Supports most languages
  - .NET, Python, Node.js, Java, and more
- Deploy static web apps
- Deploy containers (more on this later)
- No need to install/configure web server software
- Accessible via Azure portal

WebJobs

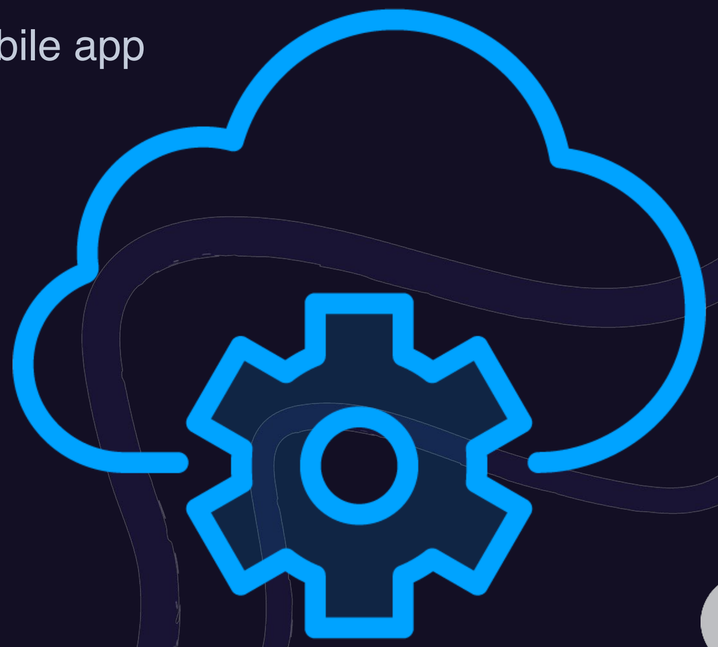
- Background tasks for application logic

API Apps

- Host your REST-based web API

Mobile Apps

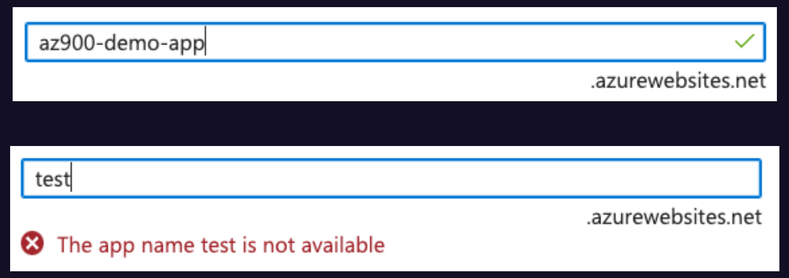
- Backend for iOS/Android apps
- Authentication, mobile app data, and push notifications



Configuring and Deploying App Service (Web App)

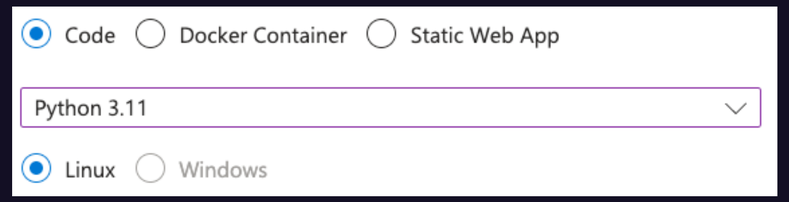
Choose a unique name

- Must be unique across all of Azure



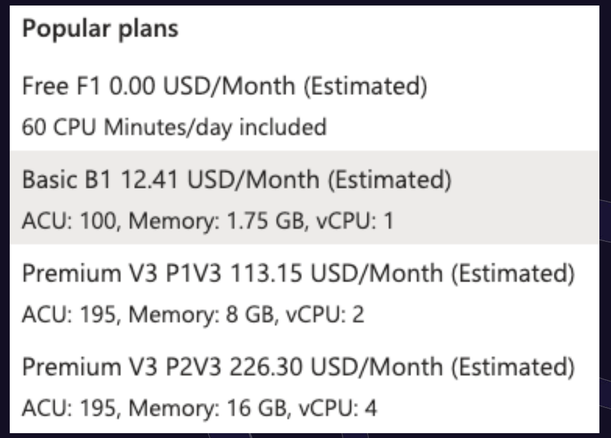
Choose publish method

- Code, container, static web app



Choose a service plan

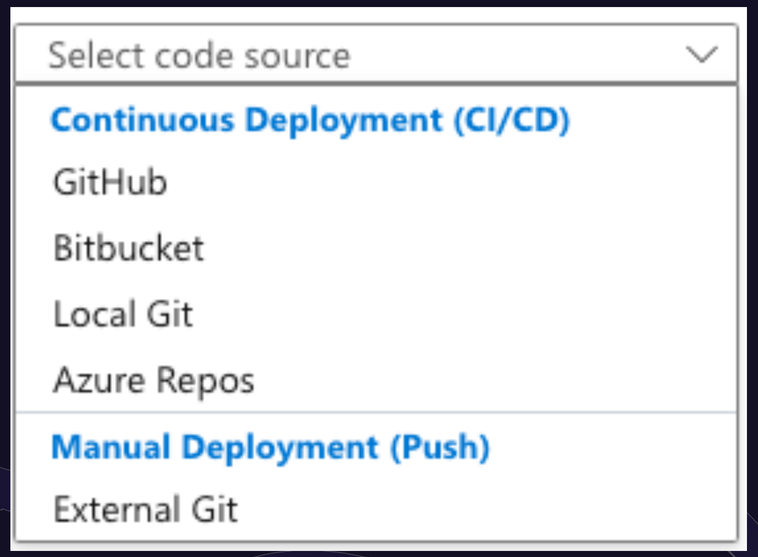
- Performance, scaling, disk space, and more

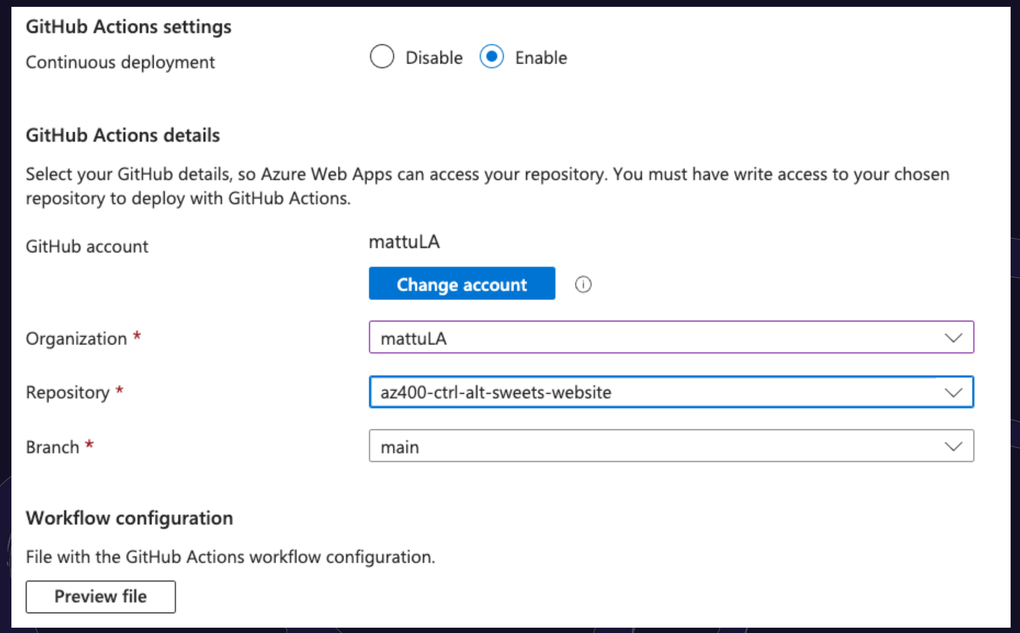


Configuring and Deploying App Service (Web App)

Deploy your code!

- Tight integration with GitHub
- Other methods work as well
- Supports Continuous Deployment for rapid iteration





Summing It Up

What is App Service?

- App hosting with minimal management overhead
- “Focus on your code, Microsoft handles the rest”
- Developer-focused product

Setting up

- Choose plan/publish method
- Deploy your code!

Demo: Creating an App Service

Matthew Ulasien
Azure Training Architect

Demo

Create App Service web app

- Python Flask

Pay attention to:

- Service plan options
- Importing code
- What we **don't** have to do compared to VMs

Summing It Up

Creating an App Service

- Naming requirements
- Streamlined process
  - Choose plan
  - Import code
  - That’s it!

Azure Functions

Matthew Ulasien
Azure Training Architect

What Are Azure Functions?

Serverless Event-Driven Code Execution

Extreme PaaS

- Practically zero management overhead

No VMs to manage

Apps only run when triggered…

- …and then they shut down until needed

What Are Azure Functions?

IaaS/PaaS

- Install your own applications
- Access to the operating system
- Resource visibility
- An app service has no OS access but has resource access

Vs.

Function

- Smallest compute service on Azure
- A single function of compute
- Called, or invoked, via a standard web address (URL)
- Runs once and stops

Architecture

VM

No maintenance

No processes

Nothing VM-related

Just focus on your functionality!

Automated Image Resizing upon Upload

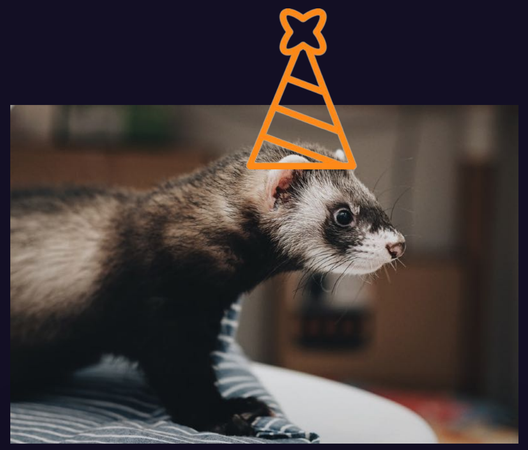


Image uploaded to website

Trigger

Goodbye!

Resize this image!

HTTP

funnyferrets.com

Function Benefits

1 Only Runs When Needed

Event-Driven
The Azure Function only runs when there is data to process. No traffic = no resource usage.

2 Saves Money

No resources running means you don't pay for the function when it is not used.

3 Resilience

If your function fails, it doesn't affect other function instances.

4 Scalability

No configuration required (no plans to choose from)
Auto-scales based on demand
Scales down to zero, and up to your determined cap

5 No Infrastructure Management

Just deploy your code…and that's it!

Summing It Up

What Is Azure Functions?

- Event-driven compute
- Only runs when triggered
- No infrastructure to manage, just deploy code

Introduction to Containers

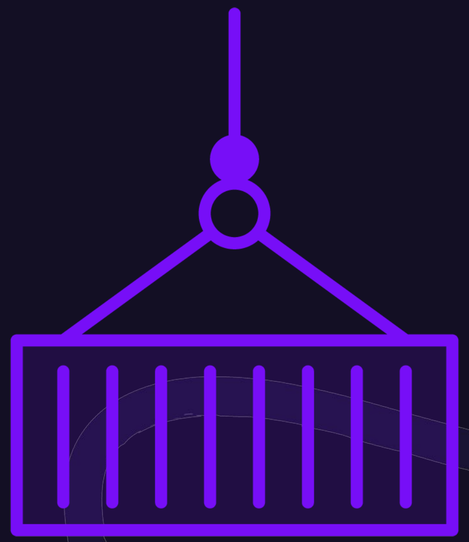
Matthew Ulasien
Azure Training Architect

What Is a Container?

Lightweight, Standalone Package for Apps

Bundled application + dependencies

- Portable, self-contained unit
- Isolated from host OS



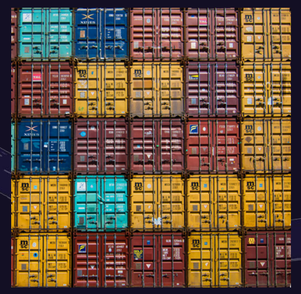
Benefits of Containers

Manage Application Dependencies

All the dependencies for an application are included in the container image.
You can manage the application and its dependencies with confidence.

Increased Portability

Applications running in containers can be deployed easily to multiple different operating systems and hardware platforms.



Consistency

The operations team can rely on containers being the same every time, no matter which target they are being deployed to.

Less Overhead

Virtual machines require a lot more maintenance and updates.
Containers don’t have any components relating to the operating system that require maintenance.

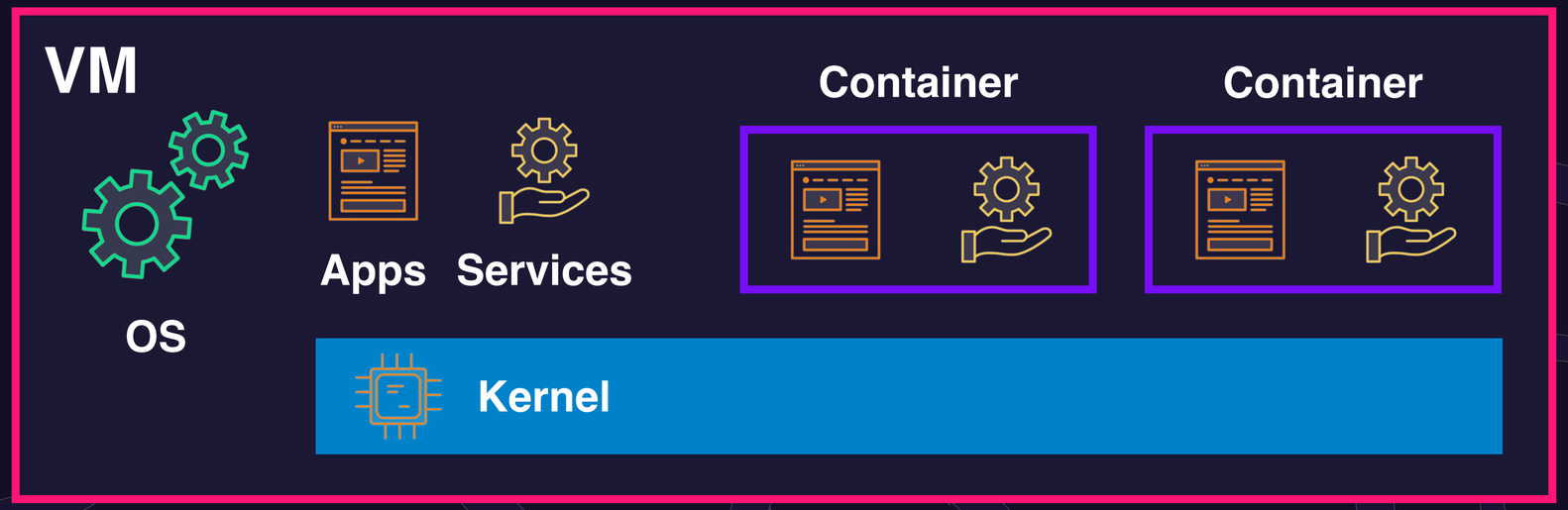
Efficiency

Development, deployment, and maintenance are all more efficient when using containers.
Scaling and patching is much simpler.

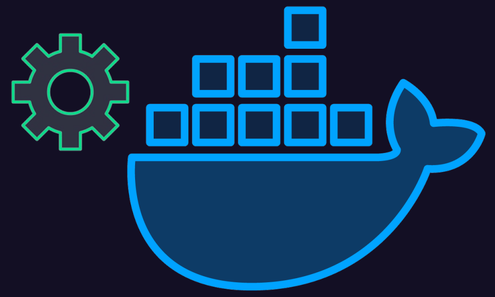
Containers vs VMs

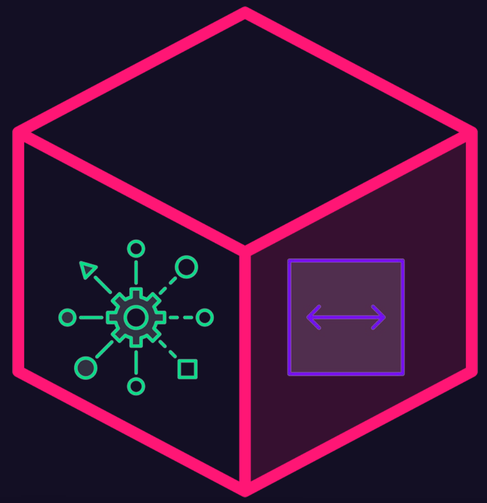
Additional layer of virtualization

- VMs: virtualized hardware
- Containers: virtualized OS
  - Build on top of host OS's kernel (core OS software)
  - Can contain only services needed for application



Container Workflow





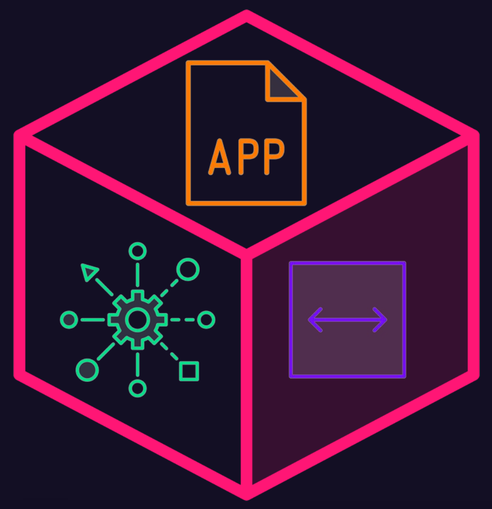
Develop Application

Application/dependencies/ execution instructions packaged in a container

Example: Docker container

Container Workflow

Develop Application



Application/dependencies/ execution instructions packaged in a container

Example: Docker container

Deploy Container

Summing It Up

What Is a Container?

- Lightweight, self-contained application package
- Portable, can run in many environments
- More portable and less resource-intensive than VMs

Container Deployment Options

Matthew Ulasien
Azure Training Architect

Container Deployment Options

Azure Container Instances (ACI)

1

On Demand = Save $$$

Use containerized applications to process data on demand, by only creating the container image when you need it. Save some cash in the process.

2

Simplicity

Minimum setup/overhead required.

Ideal for short-lived, simple workloads

3

Not as scalable

Single containers only.

No load balancing/auto-scaling.

If more scaling/complexity required for more containers, consider Azure Kubernetes Service (AKS).

Azure Kubernetes Service (AKS)

Kubernetes = Open-Source Container Orchestration

1 **Orchestrate many containers!**

Manage large-scale, high-volume, high-complexity containerized workloads

More control and customization

2 **Scalability**

Automatic scaling, load balancing, and failover

3 **More complex + higher costs**

Persistent VM nodes = $$$

Between IaaS and PaaS

Much more complex than ACI

Azure Container Apps

1 **In between ACI and AKS**

Rich Kubernetes features

Fully managed - simplified management

2 **Serverless and scalable**

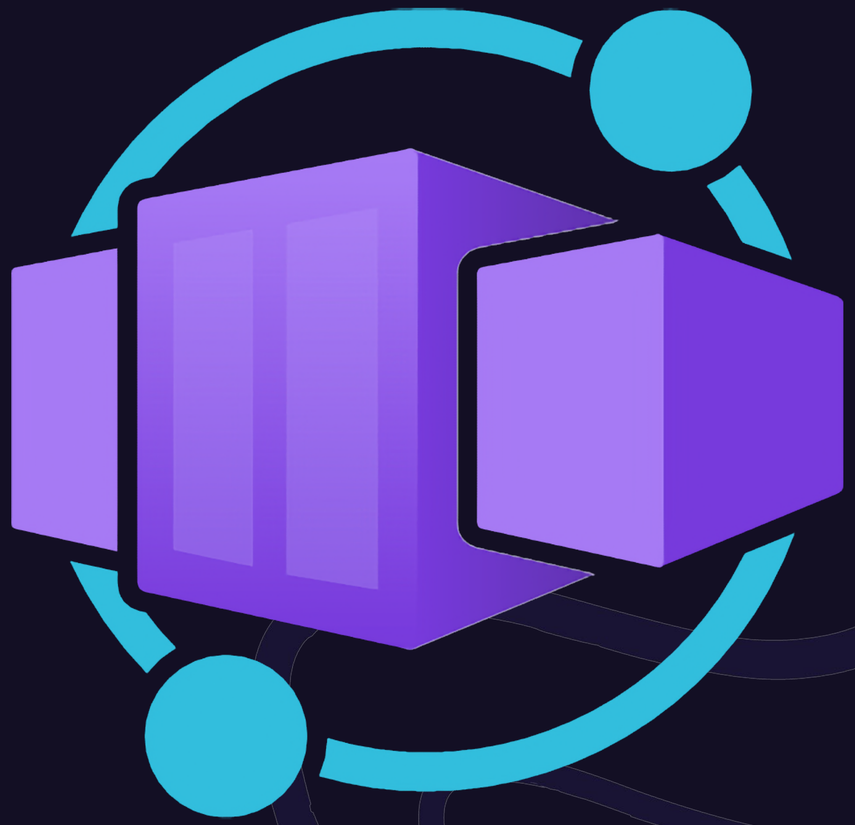
Ideal for serverless microservices

Auto-scaling enabled

3 **Not quite as powerful as AKS**

No access to Kubernetes APIs

Less customization



Other Deployment Options

Virtual Machines

You can do ANYTHING with VMs

Much more to install/manage/configure

Azure App Service

Ideal for long-running web applications

Use any programming language

Azure Functions

Containerized event-driven applications

Like App Service, use any programming language

Summing It Up

Azure Container Instance

- Fastest/easiest way to deploy a single container
- Limited power/flexibility

Azure Kubernetes Service

- Greatest amount of control/scaling/flexibility
- Higher cost and complexity

Azure Container Apps

- Best of both worlds
- Not quite as much customization as AKS

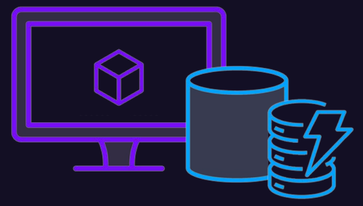
Exam Tips: Azure Compute

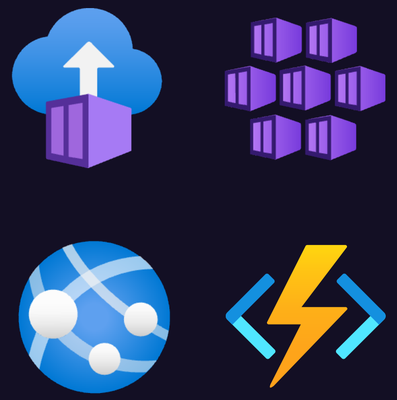
Matthew Ulasien
Azure Training Architect

Exam Tips: Azure Compute

Compute Options - Flexibility vs. Easy Management

Virtual Machines





IaaS

- Greater customization/control
- More management overhead

PaaS

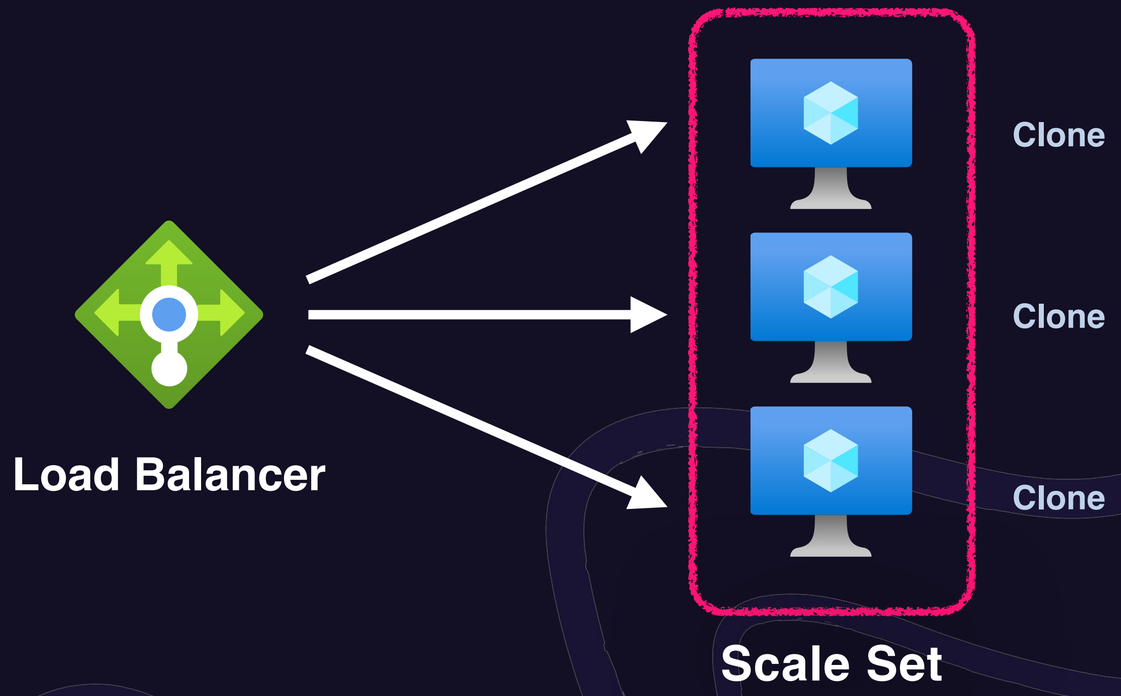
- Less customization/control
- Less management overhead

VM Scale Sets

Auto-scaling Groups of Identical VMs

Multiple identical VMs

- All managed from the same place
- Auto-scale based on load/metrics
- Behind a load balancer
- Can deploy across zones in single region

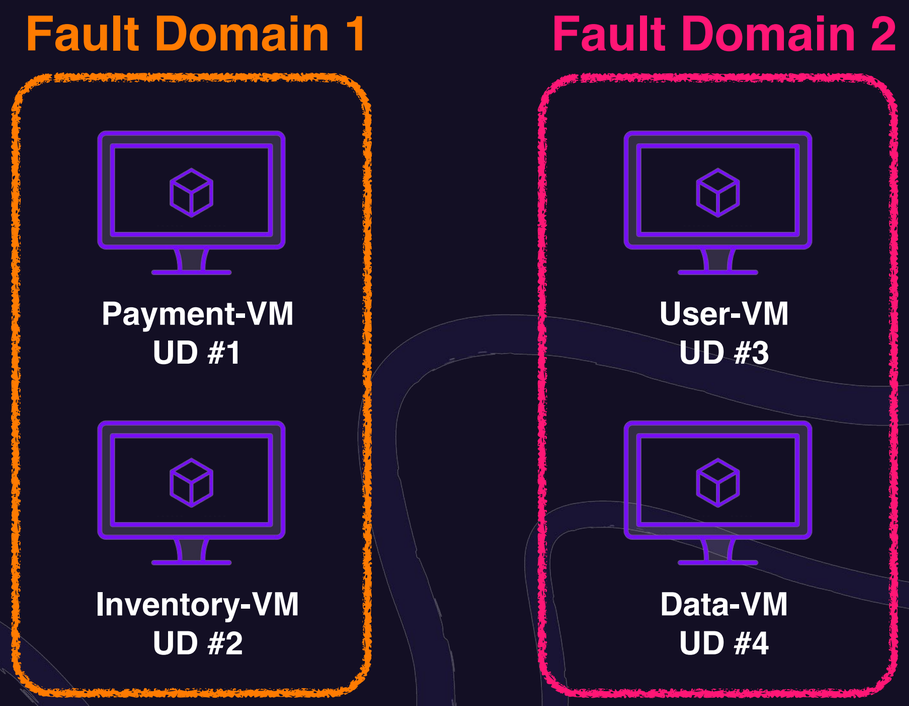


Availability Sets

High Availability for Unique VMs in Single Zone/Datacenter

Spread assigned VMs across update and fault domains

- **Fault domain:** Server rack with shared power/networking
- **Update domains:** Hypervisor groups on same maintenance schedule



Azure Virtual Desktop

Virtualized Windows Desktops and Apps, Hosted on Azure

- Ideal for remote work and/or secure data handling
- **Centrally managed** and **secured**
- Data stays in Azure

PaaS Compute Services

Know Each Service's Use Case

Long-running
web applications

Azure App Service

Single containers
Easy to deploy

Azure Container Instances

Short-life, event-driven
applications

Azure Functions

Many containers
More control + complexity

Azure Kubernetes Service

Azure Virtual Networks

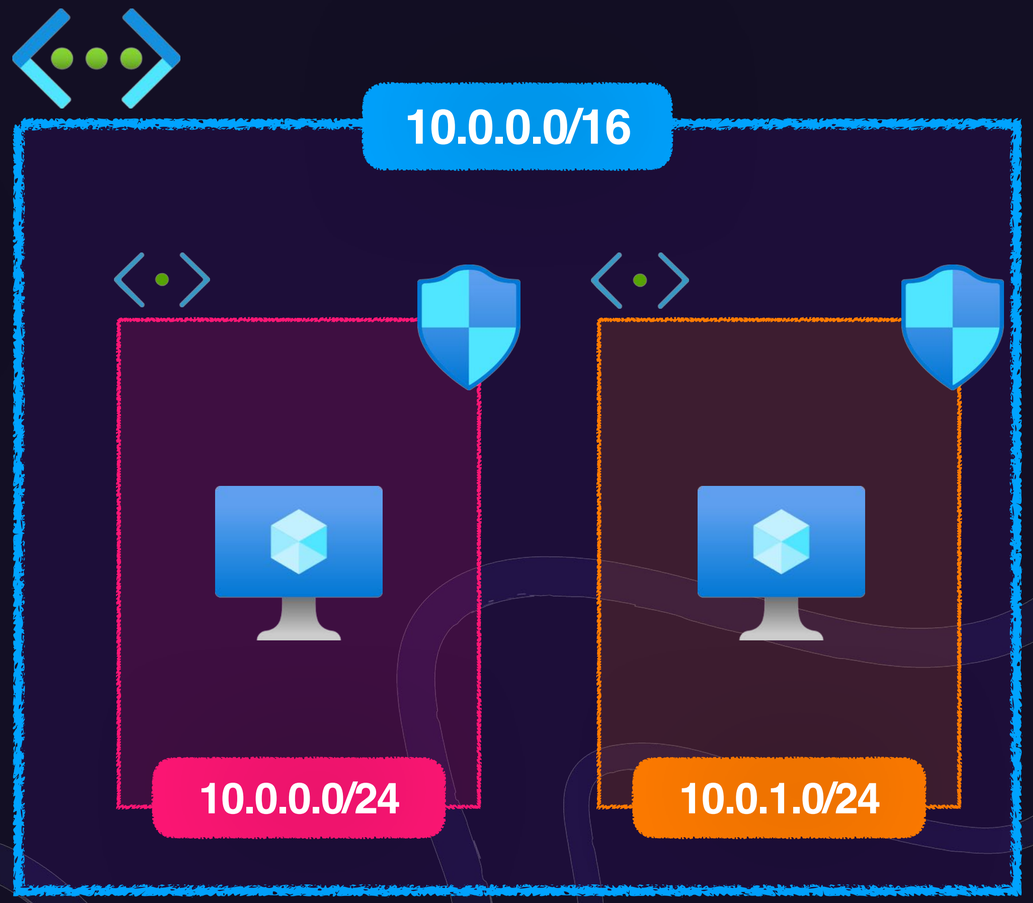
Matthew Ulasien
Azure Training Architect

Virtual Network (VNet): The Core of Azure Networking

Private, Isolated Network in Azure

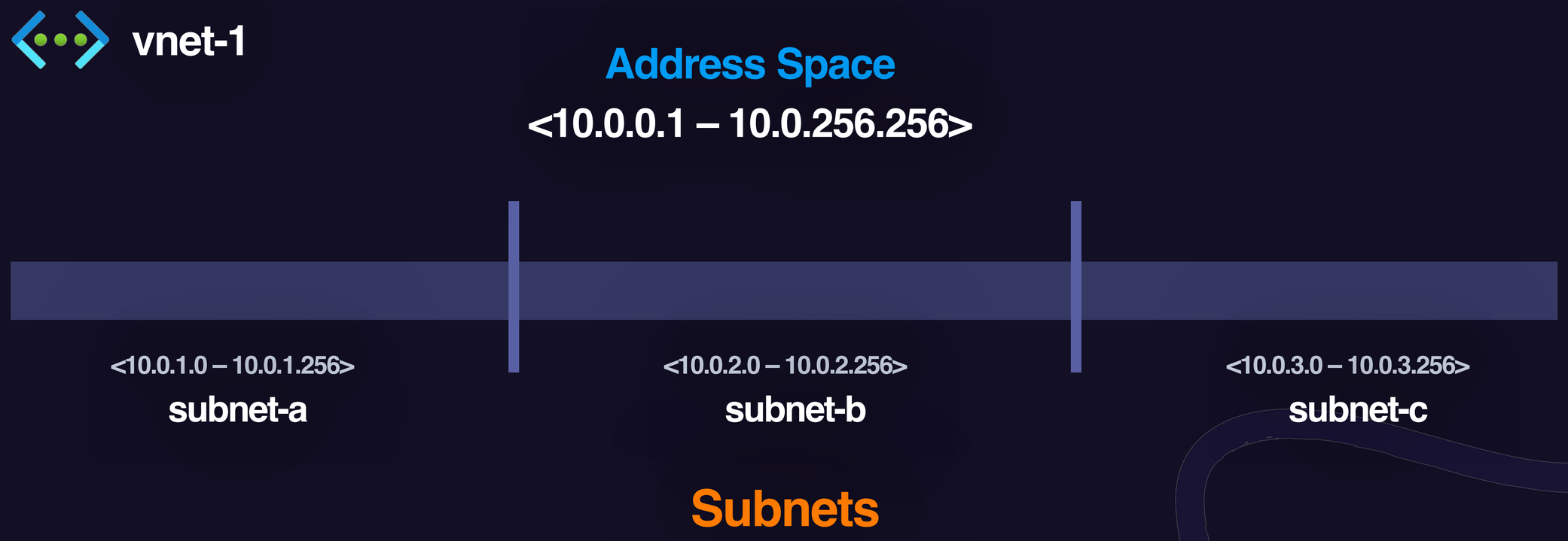
- Home for all VMs
- VM isolation/communication boundary
- Private and public networking
- One or more address spaces

  Each **address space** contains one or more **subnets**.



Address Spaces and Subnets

Address Space: VNet's overall IP range



Subnets: Segmented, smaller IP ranges within address space

Address Spaces and Subnets

Subnets

1. **Resource Grouping**

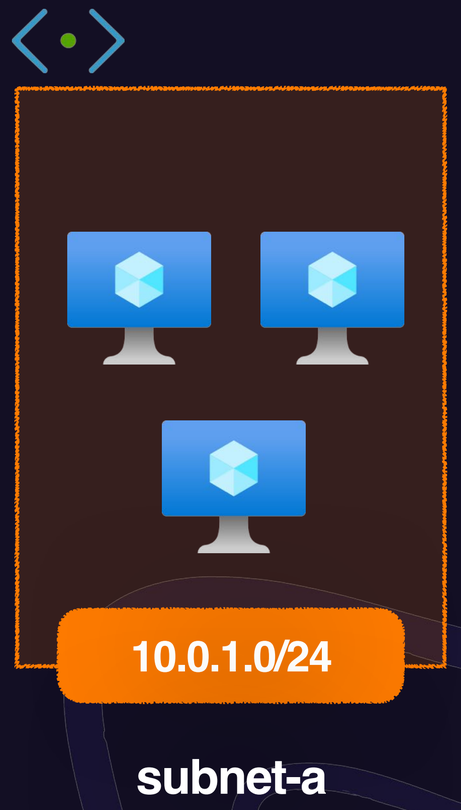
   Group resources onto the same subnet to make it easier to keep an overview.

2. **Address Allocation**

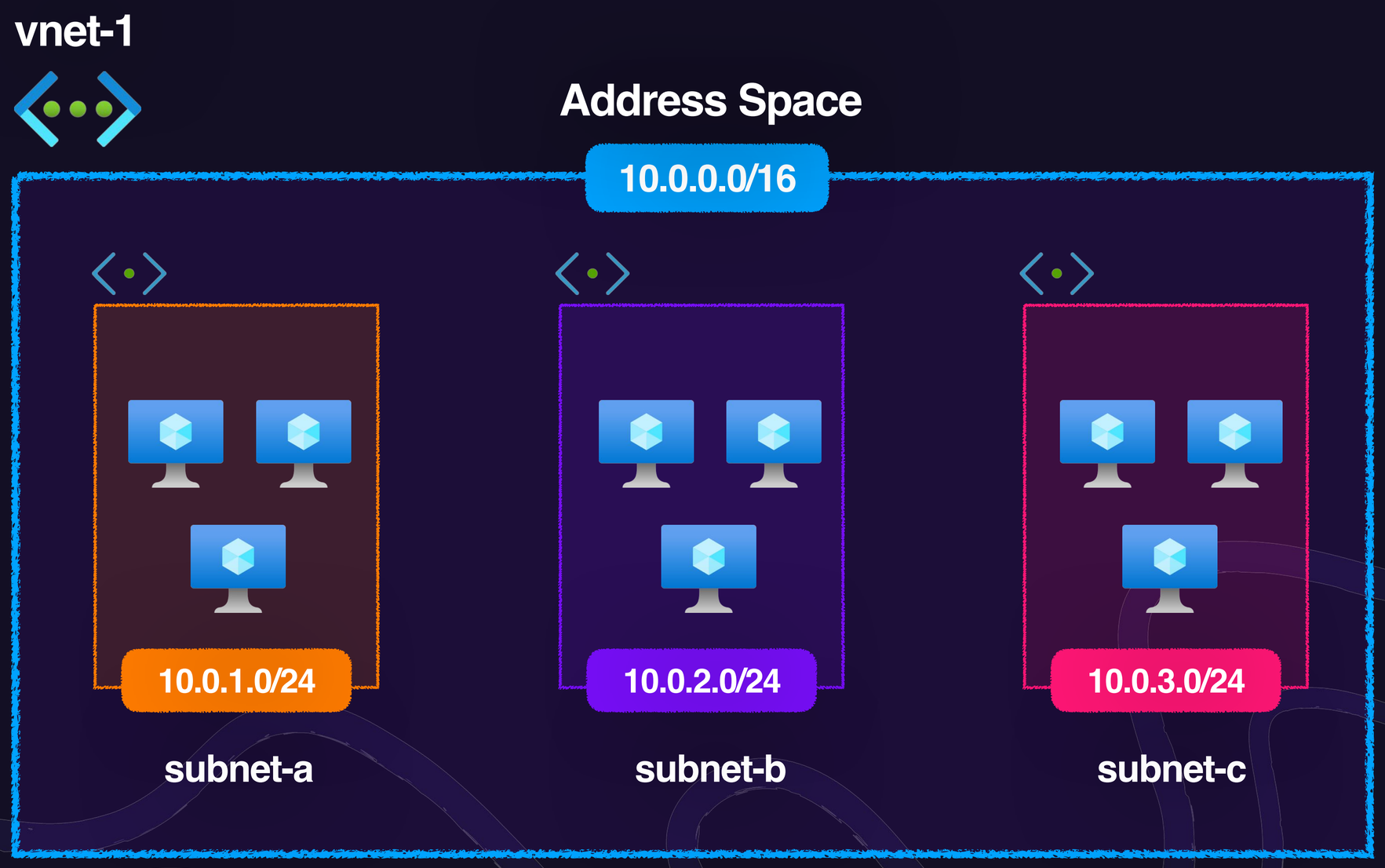
   More efficient to allocate addresses to resources on a smaller subnet.

3. **Subnet Security**

   Use network security groups to secure individual subnets.



Address Spaces and Subnets in Practice



What Is an IP Address?

Unique Identifier for Network Devices

Send to:

123 Smith Street
Guru Square

142.56.98.214

Destination:

123 Smith Street
Guru Square

142.56.98.214

Private IP: Local network identifier

Invisible to outside world

10.0.0.0 - 10.255.255.255 (10 /8 prefix)

172.16.0.0 - 172.31.255.255 (172.16 /12 prefix)

192.168.0.0 - 192.168.255.255 (192.168 /16 prefix)

Public IP: Global network identifier

Accessible to outside world

Example: Public website

VM IP Configurations

Public vs. Private

Private IP required, public optional

Static vs. Dynamic Public IP

Dynamic: **Public** IP **changes** upon VM deallocation/reallocation.

Static: **Public** IP remains upon VM deallocation/reallocation.

VNet Regions and Subscriptions

Regions

A VNet belongs to a single region. Every resource on the VNet must be in the same region too.

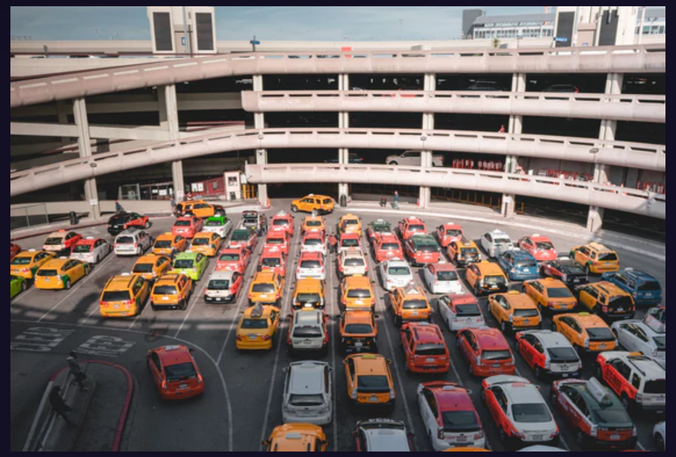
Subscriptions

A VNet belongs to just one subscription, but a subscription can have multiple VNets.

Cloud Advantages

Software Defined Networking

Network components are software configurations
No physical constraints - network is virtualized



Scaling

Adding more VNets or more addresses to one is simple.

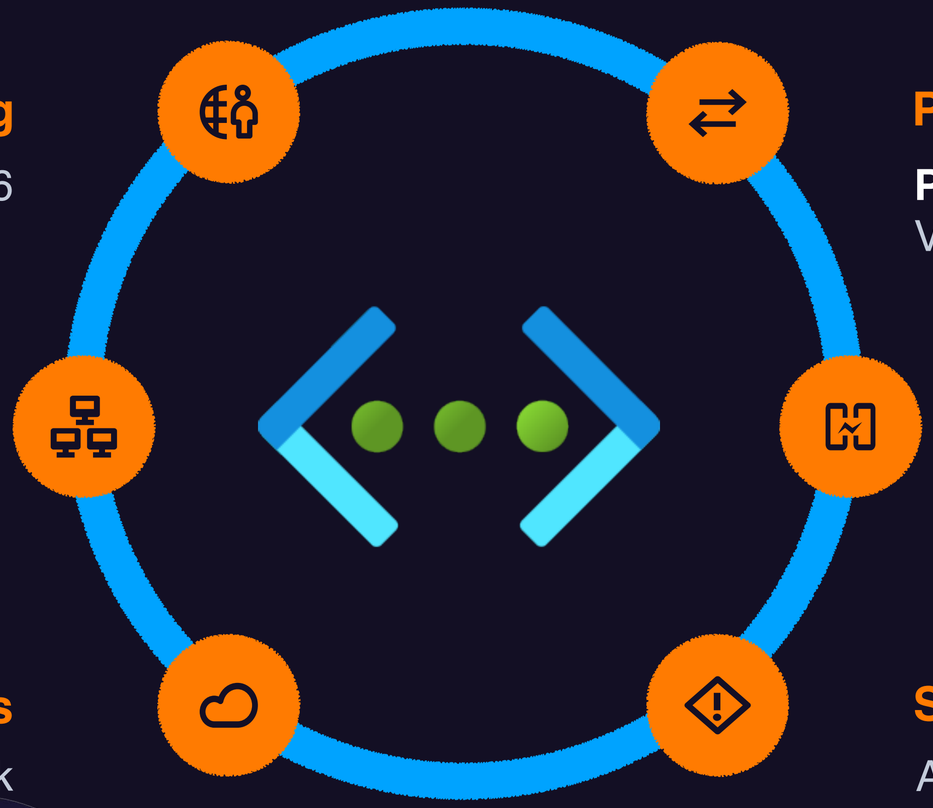
High Availability

Peering VNets, using a load balancer, or using a VPN gateway all increase availability.

Isolation

Manage and organize resources with subnets and network security groups.

VNet: Communication Nerve Center



Public Networking

Public IP address IPv4 and IPv6

Peering

Private peering between Azure VNets

Intra-VNet

Communicate **privately** with other VNet resources

Hybrid Networking

Private networking with on-prem or other clouds

Managed Services

Public and private network communications

Security

All communications can be filtered
- Network security groups (NSGs)
- Azure Firewall

Key Takeaways

Virtual Network = Core Network Building Block

Central construct for private and public communications

IP Addressing

- VMs must have private IP, public optional
- Dynamic vs. static public IPs
  - Dynamic: Changes after de/reallocation
  - Static: Permanent public IP (at extra cost)

VNet Structure

VNets bound to a region

- One or more address spaces
- Subnet(s) contained in address space

Multiple Communication Options

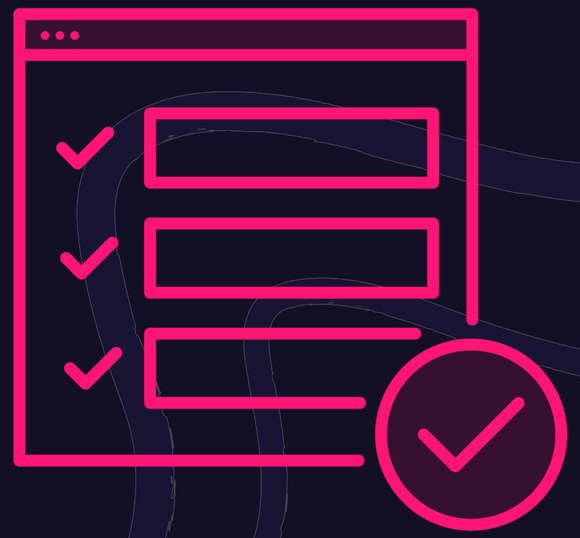
- Public
- Within VNet
- Hybrid
- Peering (to other VNets)
- Managed services

Network Security

Matthew Ulasien
Azure Training Architect

Exam Scope

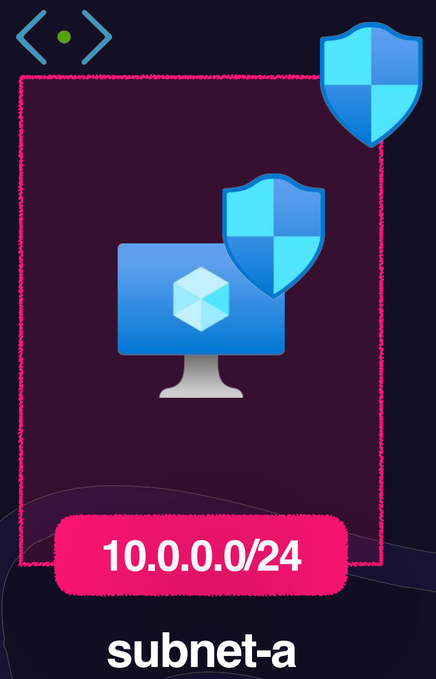
- Security topics not on current version of AZ-900 exam
- However, still fundamental topics to cover for networking



Network Security Group (NSG)

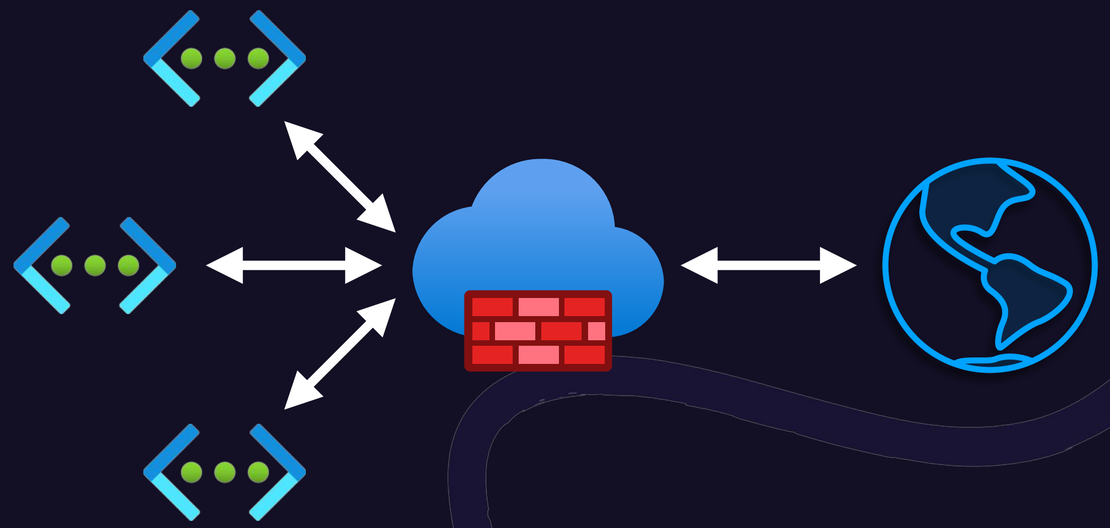
Primary traffic filter for subnets/VMs

- **Applied to subnet or individual VM**
- **Free service**
- **Granular rules for fine network control**
  - Inbound/outbound filters
  - Traffic types (TCP/UDP ports, ICMP)
  - Allowed sources/destinations
  - Allow or deny multiple types of traffic
  - Priority of overlapping rules
- **Example: Only allow RDP (TCP:3389) access from corporate office**



Advanced Firewall Services for Multiple Networks

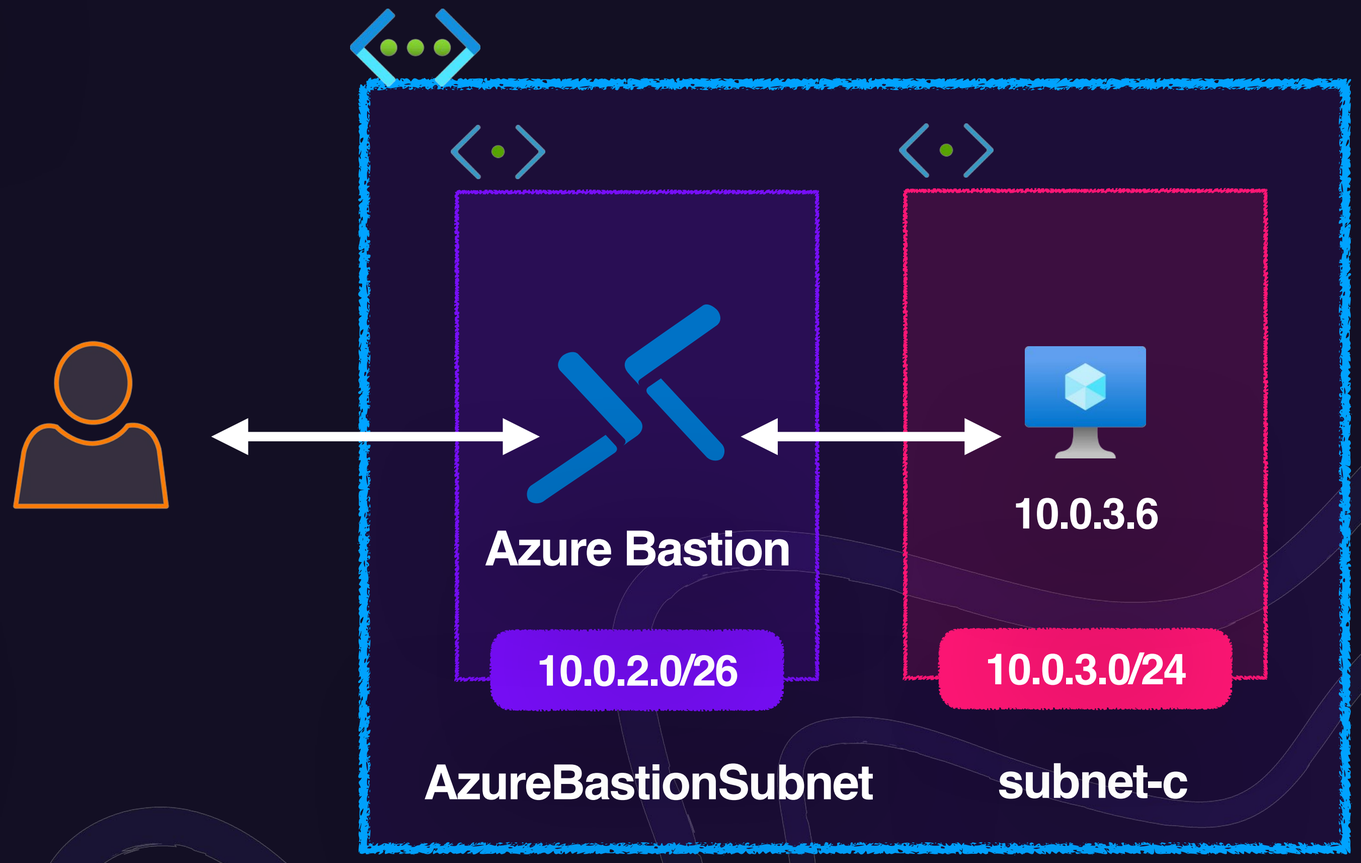
- Centralized traffic control for multiple VNets
- Paid service
- More advanced than NSGs
  - Threat Intelligence
  - Advanced filtering rules
  - URL filtering
  - DNS proxy
  - On-premises network integration



Azure Bastion

Secure SSH/RDP access for private VMs

- **Connect to VMs with no public IP**
  - Managed ‘jump server’
- **Fully managed service**
- **Deployed to VNet**
  - Specific subnet name required
- **Connect via RDP/SSH via web browser or native client**



Network Peering

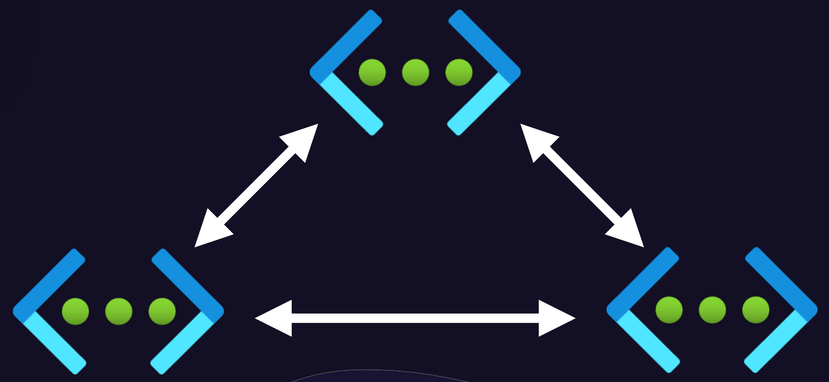
Matthew Ulasien
Azure Training Architect

Challenge: Connecting Multiple VNets

Connect multiple VNets to act as single network

Extend private networking to other Azure regions

Keep all traffic on Microsoft backbone



Solution: Virtual Network Peering

Big Picture: Virtual Network Peering

Private connectivity across Azure VNets

1. **Expand Azure Network Private Connectivity**

   Extend connectivity across multiple VNets

2. **Secure Traffic**

   All traffic stays on Microsoft's private backbone

3. **Extend reach**

   Peer across regions, subscriptions, and tenants

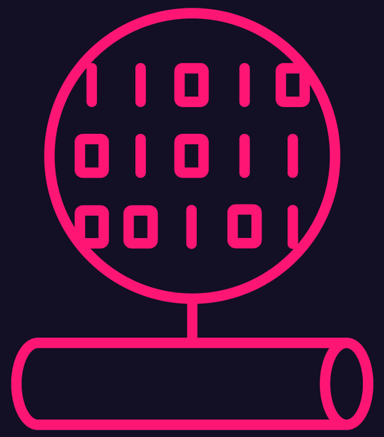
Network Peering

Key Benefits

Speed

Low latency

Maximum bandwidth allowable per VM



Traffic Privacy

Traffic stays on Microsoft private backbone

Not exposed to public internet

Control Traffic between VNets

Network security groups

Custom routes

Scenario: Multi-national Presence

E-commerce company expansion

Headquartered in North America

Expanding Azure presence to London and Tokyo

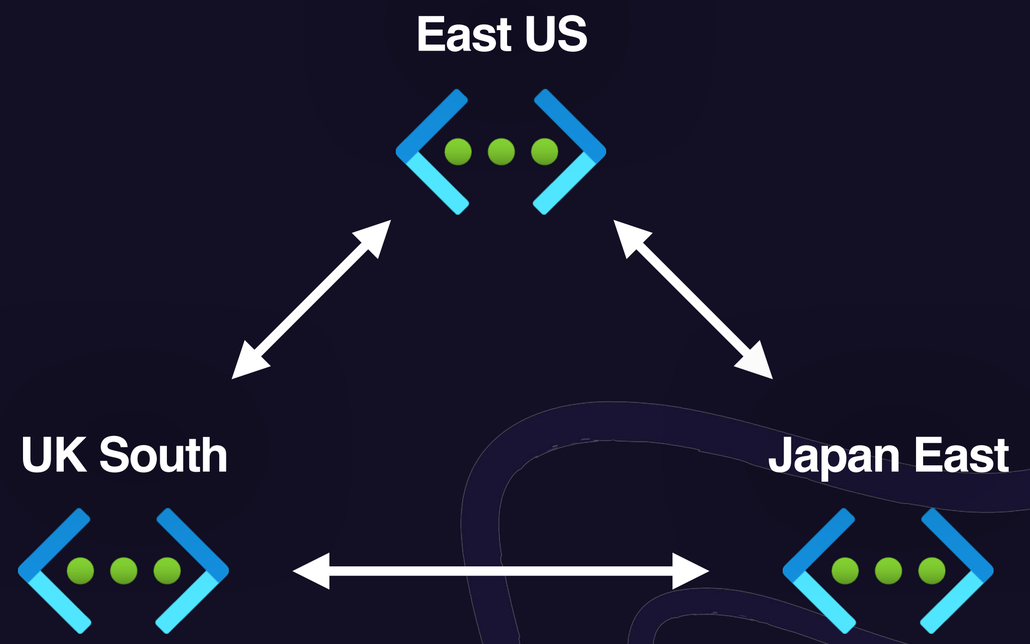
Need to sync data between regions

Inventory, user data, analytics

Peering synchronizes data quickly and securely

Traffic stays on private backbone

Update data in real time



Demo: Creating a Virtual Network

Matthew Ulasien
Azure Training Architect

Demo

Create an Azure Virtual Network

Create two subnets

Create a new VM and add to VNet

Pay attention to:

- Subnet spaces inside of address space
- Regional requirements for added VMs

Summing It Up

Creating a Virtual Network

- Must have:
  - Address space
  - Subnets inside of address space

Bound to single region

- VMs must be in the same region

Azure DNS

Matthew Ulasien
Azure Training Architect

What Is Domain Name System (DNS)?

Translates domain names to IP Addresses

"The phone book of the internet"

Public or private "phone book"

Public or private network/IP translation

If DNS stops working… everything stops working!

Memorize IP for every site? ☹️

Use easy-to-remember names? 😁

microsoft.com = 104.215.148.63

It's not DNS
There's no way it's DNS
It was DNS

DNS Resolution Basics

Connection request resolved by DNS host/server

“Who can tell me the IP address of microsoft.com?”

“microsoft.com is 20.231.239.246”

DNS Host

Public vs. Private DNS Resolution

- Public = public domain registrar —> authoritative name server

"I am the global authority that says microsoft.com is 20.231.239.246."

Authoritative DNS Name Server (Host)

- Private = private DNS server/host

Private DNS server

Azure Public and Private DNS Services

Azure DNS Zones

Public DNS resolution

Use Azure as authoritative name server

Azure Private DNS Zones

Custom DNS resolution within VNets

Global services, not tied to a single region!

Benefits of Azure DNS Services

- Uses the same tools/credentials/billing as other Azure resources
- RBAC for access management
- Activity monitoring
- Resource locks to prevent changes

Hybrid Networking

Matthew Ulasien
Azure Training Architect

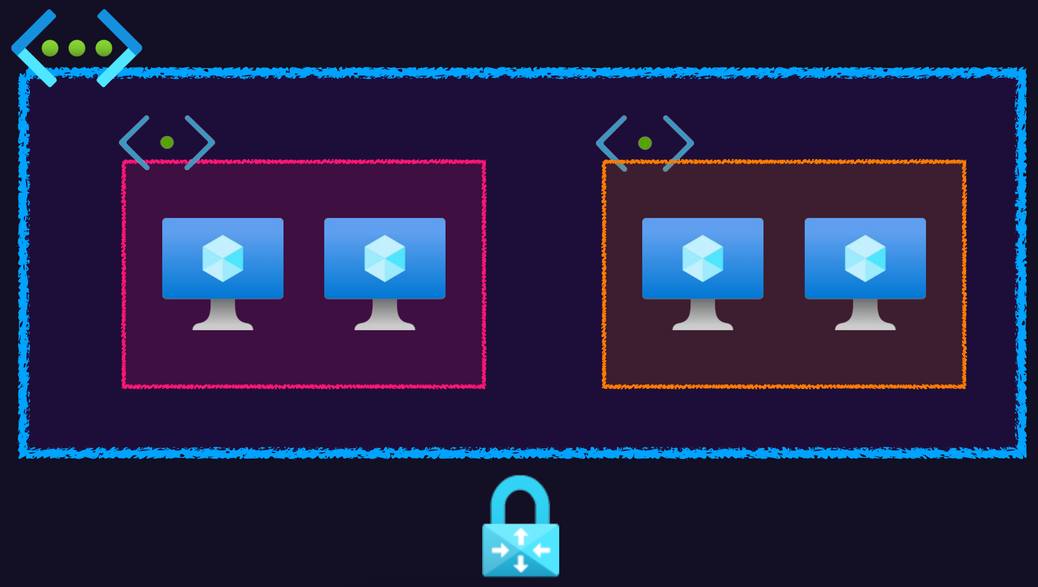
Review: What is Hybrid Networking?

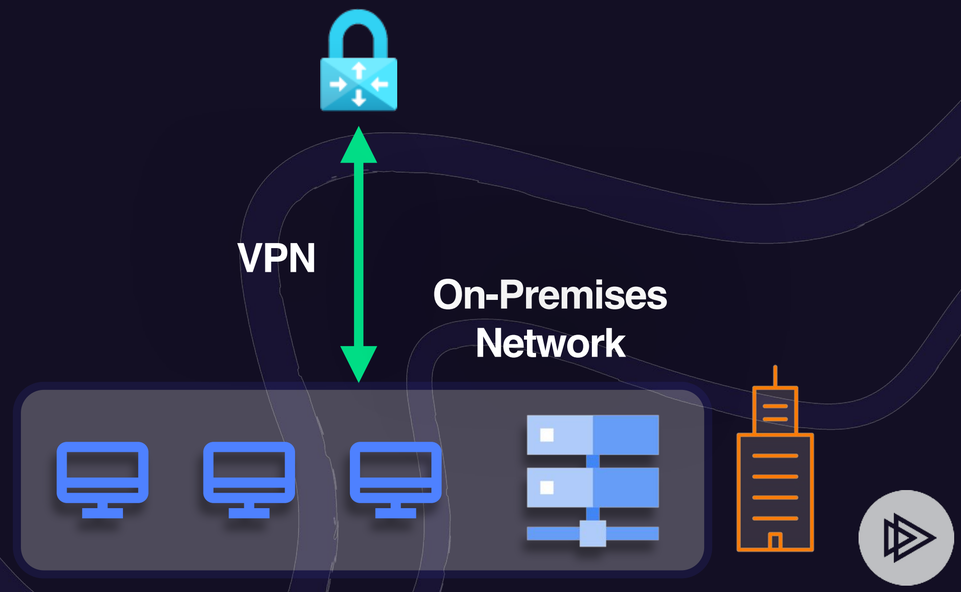
Connect trusted external networks over private IP networking

On-premises

Other cloud networks (e.g., AWS, GCP)

Other Azure VNets





Hybrid Connectivity Benefits

Extend private networking beyond your VNet

Encrypt traffic between networks

Azure Hybrid Connection Options

Site-to-Site (S2S) VPN

- Network-to-network
  - Requires remote public-facing router
- Connect over IPsec/IKE
- Uses public internet
- Can connect to other Azure VNets

ExpressRoute

- Direct, private connection to Microsoft services (including Azure)
  - Not over public internet
- Lease dedicated line from carrier

Point-to-Site (P2S) VPN

- Azure network to individual computer
- Ideal for telecommuters
- Also over public internet

Virtual Network Gateway

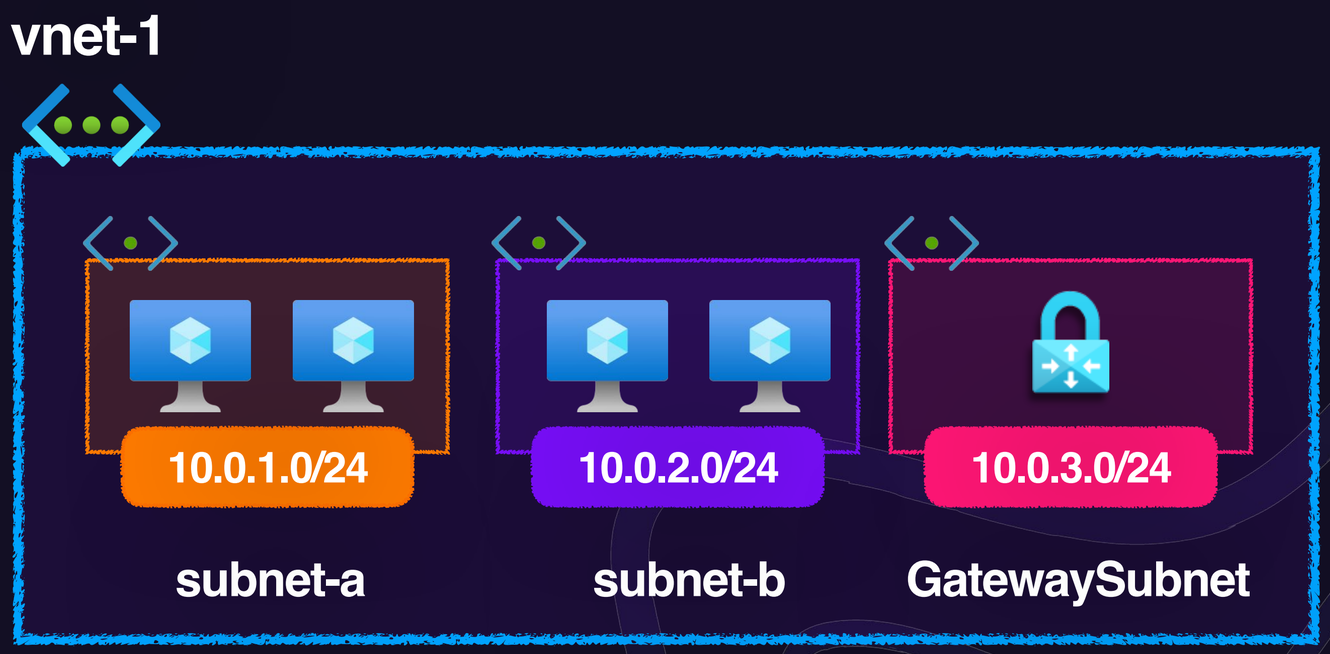
Core component of all Azure hybrid connectivity solutions.

Managed Azure resource hosted in VNet

Dedicated subnet with specific name

Endpoint connecting VNet and hybrid connection option

One Network Gateway per VNet

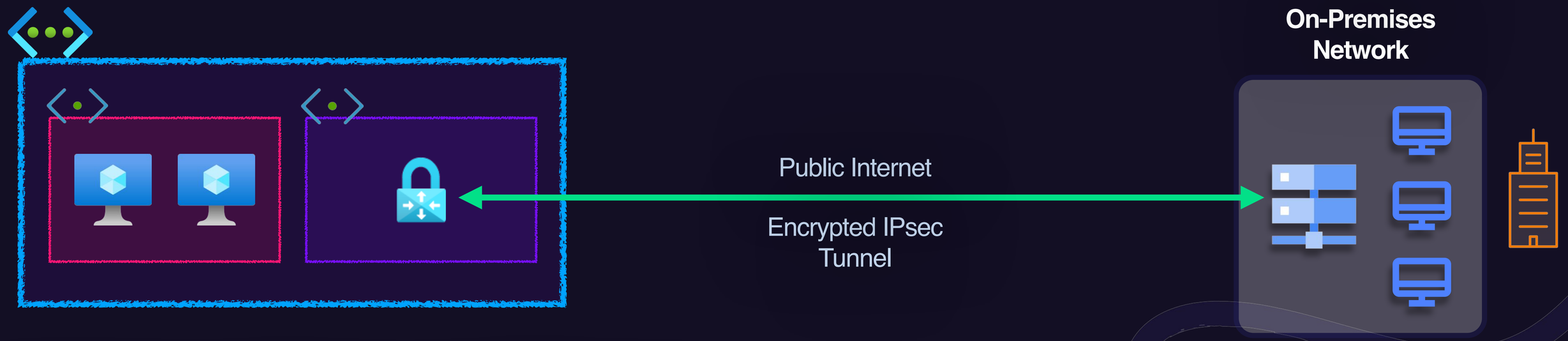


Azure VPN

Matthew Ulasien
Azure Training Architect

Site-to-Site (S2S) VPN

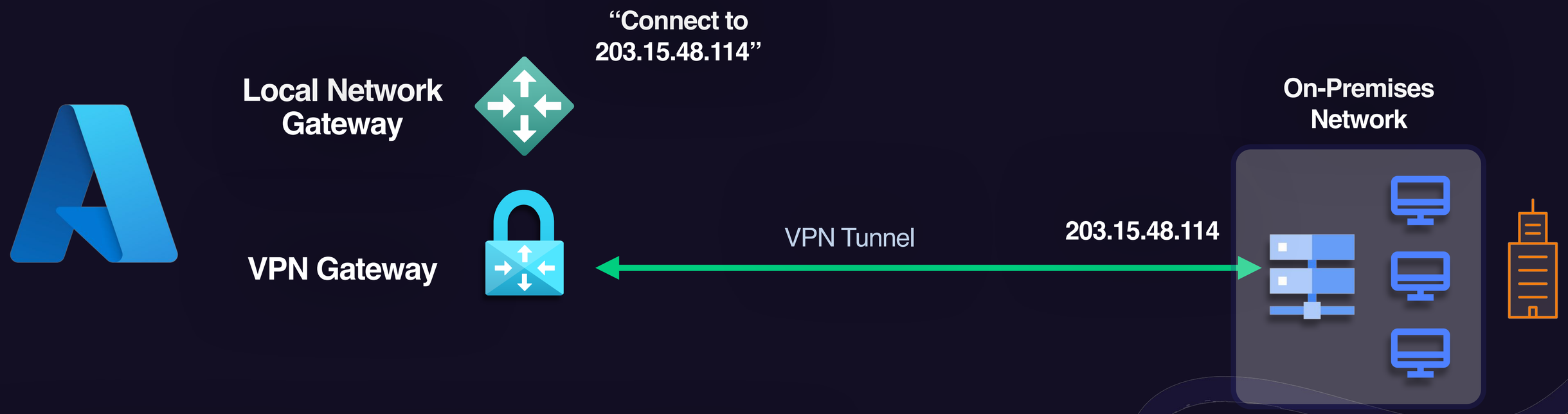
Encrypted Network-to-Network Connection over Public Internet



VNet Gateway + VPN becomes a “VPN Gateway”

Azure VPN

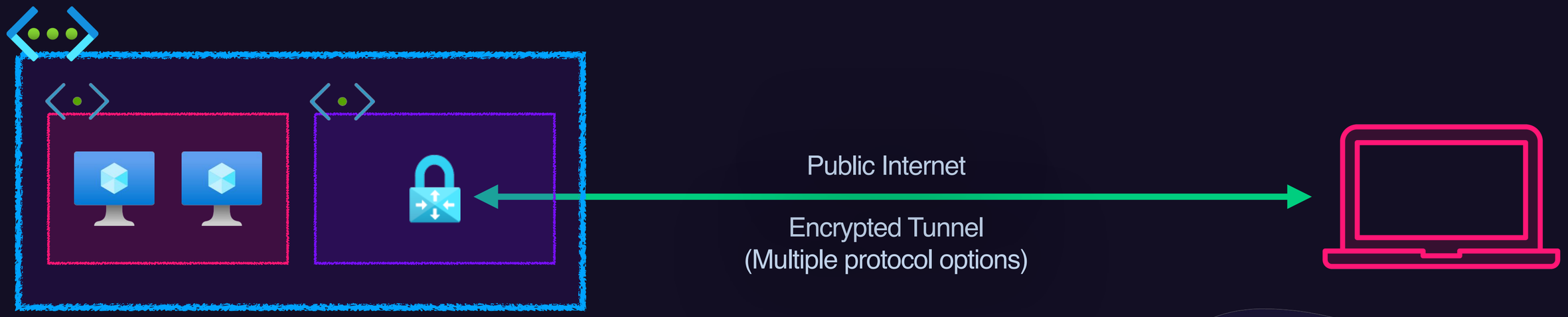
S2S VPN Components



Local Network Gateway = Remote network configuration

Point-to-Site (P2S) VPN

Encrypted Network-to-Device Connection over Public Internet



Ideal for remote works who need private networking access to VNet resources

VPN Types: Policy-Based vs. Route-Based

Policy-Based

- Most backwards compatible
- Static routing
- No Point-to-Site VPN
- Connect to single site

VS

Route-Based

- Not as backwards compatible
- Dynamic routing
- Supports Point-to-Site VPN
- Connect to multiple sites

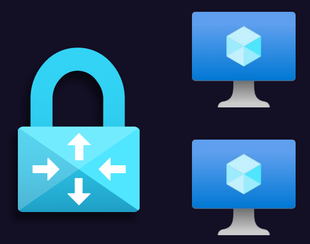
Route-based is always the better option if supported!

Policy-based is more backwards compatible

VPN and High Availability

Behind the scenes…

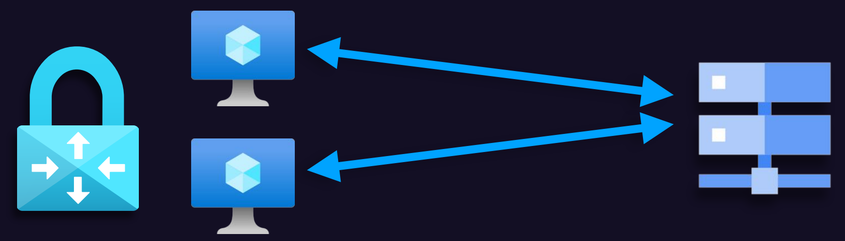
Gateway = two managed VMs running connection



Active-Standby

Default configuration = one VM running one tunnel

If one VM fails, other takes over after slight delay

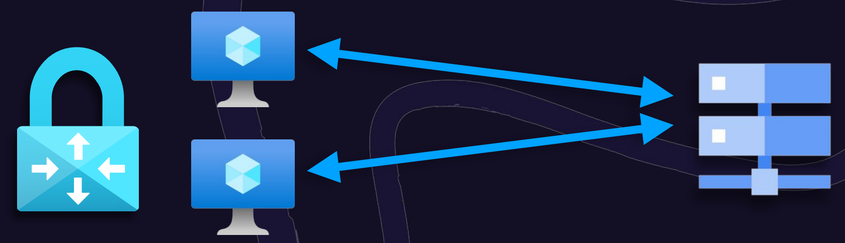


Active-Active

Two active tunnels

Maximum high availability

Additional configuration requirements



Peering vs. VPN to connect Azure VNets

Peering

- No encryption between networks
- Traffic stays on Microsoft backbone
- Lower latency
- Maximum bandwidth between networks
- Less expensive, less to manage

VS

VPN

- Provides encryption between networks
- Involves public internet
- Network gateway manages traffic
- Bandwidth limited, more hops
- Ideal for security and compliance (encryption)
- Network gateway = additional costs

Azure VPN

Key Takeaways

VPN Options

Site-to-Site (S2S) = ‘Network-to-Network’

Point-to-Site (P2S) = ‘Network-to-Computer’

VPN Types

Route-based = more capabilities

Policy-based = more backwards compatible

S2S VPN Components

Virtual Network Gateway

Gateway Subnet

Local Network Gateway = Remote configuration info

High Availability

Active-Standby = One active tunnel

Active-Active = Two active Tunnels

Peering vs. VPN for VNets

Peering = faster, cheaper, and stays on MS backbone

VPN = encrypted, but slower and more expensive

ExpressRoute

Matthew Ulasien
Azure Training Architect

What Is ExpressRoute?

Private, Fast Connection to Microsoft Cloud

Private, leased lines into Microsoft's network

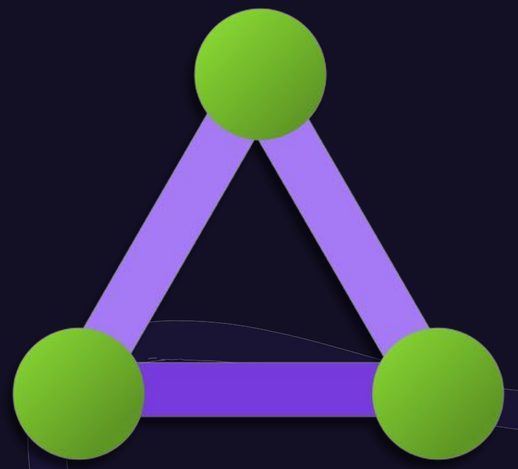
- Not over the public Internet
- On-premises connections only

Often partner with connectivity provider

Privately connect to VNets AND other Microsoft Cloud services

Benefits:

- Reliable and fast
  - Built-in redundancy (active-active)
- High-speed options available (up to 100Gbps)



Remember: Not just for VNets

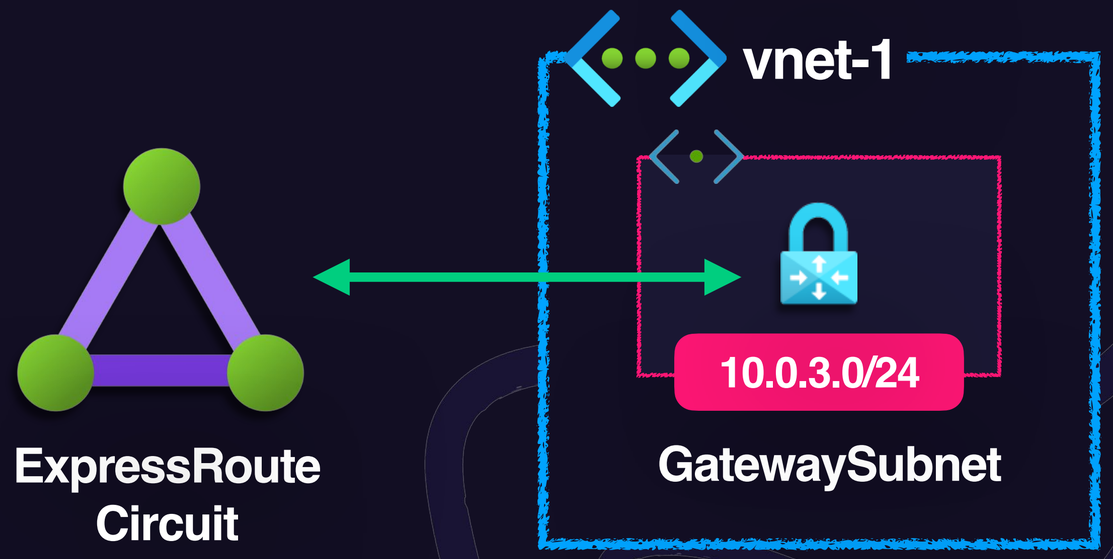
Same Virtual Network Gateway as VPN

Same subnet naming requirement

However, configured as ExpressRoute Gateway vs. VPN Gateway

Gateway connects to ExpressRoute Circuit

ExpressRoute Circuit = Azure resource connecting to private connection



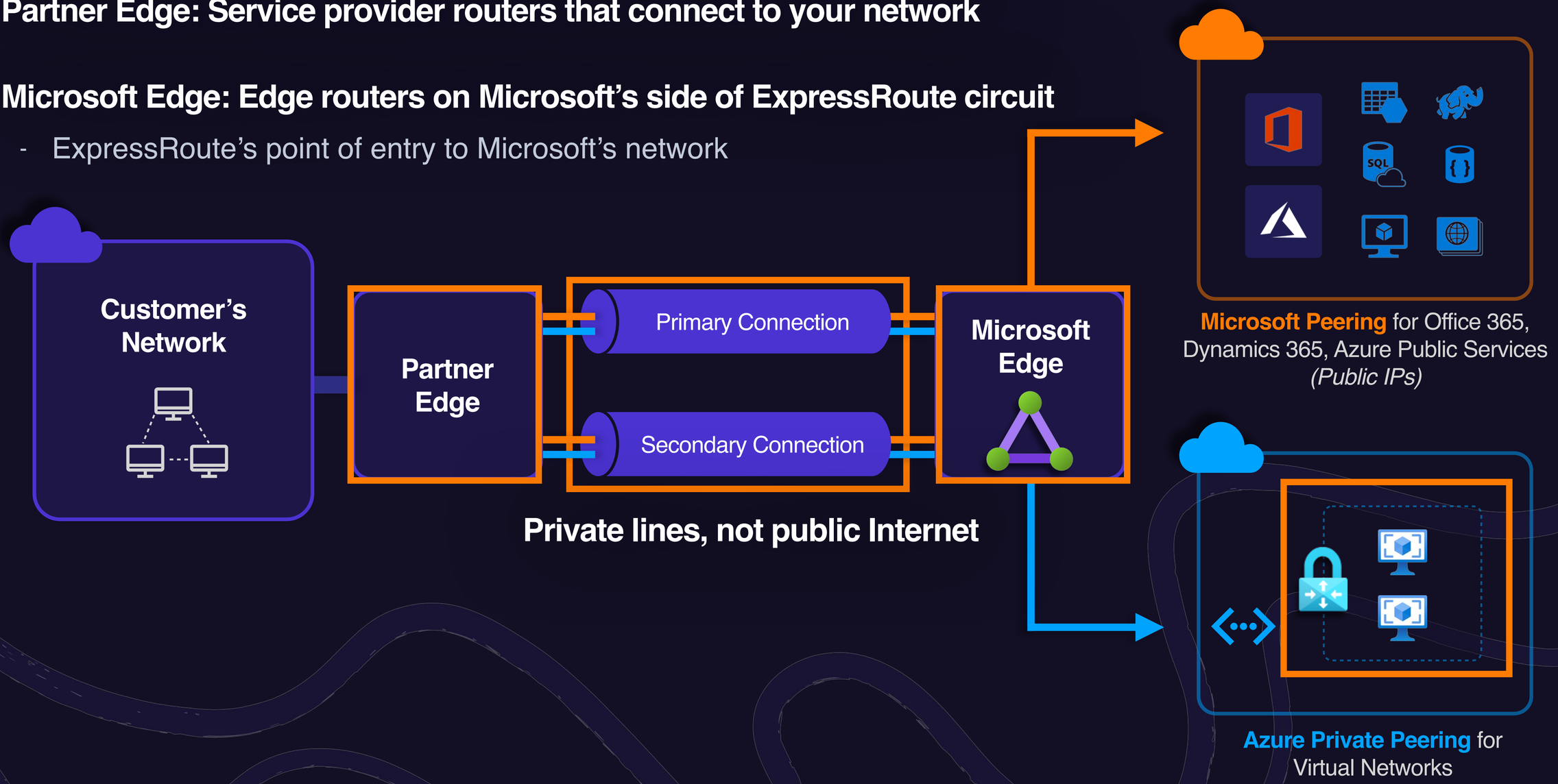
ExpressRoute

Broad ExpressRoute Infrastructure

Partner Edge: Service provider routers that connect to your network

Microsoft Edge: Edge routers on Microsoft's side of ExpressRoute circuit

- ExpressRoute's point of entry to Microsoft's network



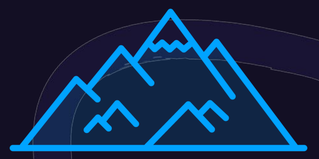
ExpressRoute Compared To VPN

ExpressRoute is…

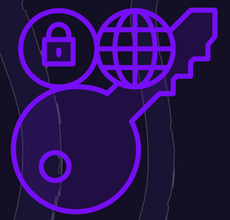
1. **Faster**
   Up to 100 Gbps

2. **Costs more**

3. **More permanent**



4. **Private**



Public and Private Endpoints

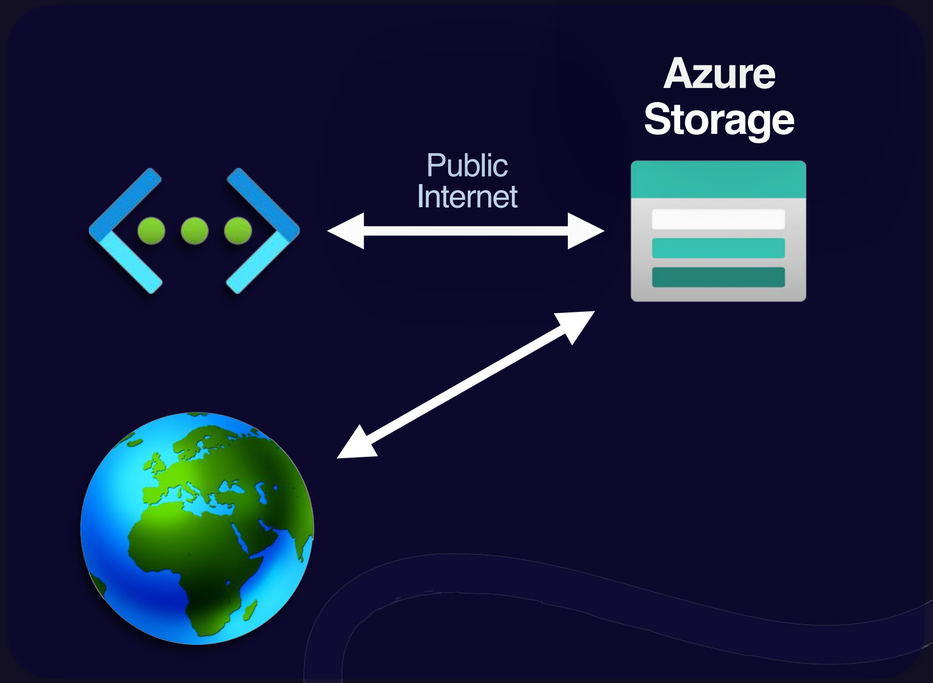
Matthew Ulasien
Azure Training Architect

Public Endpoints = Publicly Reachable PaaS Services

DEFAULT:

Managed (PaaS) services reachable over the public internet

- Virtual network —> PaaS over public internet
- Also exposed to the public
- Problem with sensitive resources



What if we want to limit or remove public exposure?

SOLUTION:

Remove public endpoint/Enable private networking

- **Private endpoints**

Private Endpoint: Private Connection to PaaS Service

Managed network interface

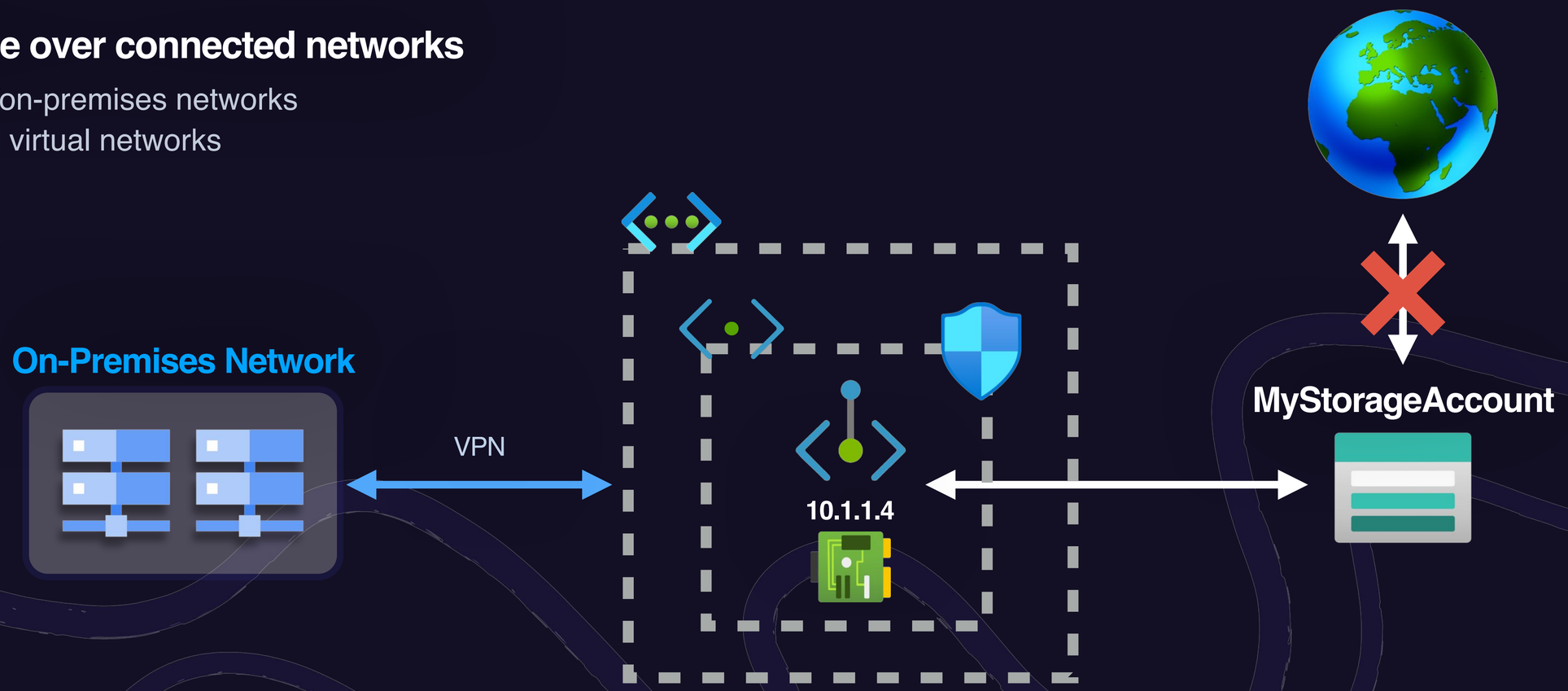
- Private connection to specific instance of a service
- e.g., single storage account, SQL instance, etc.

Can completely disable public access to a connected service

- Truly private
- Public endpoint disabled

Available over connected networks

- Hybrid/on-premises networks
- Peered virtual networks



Scenario

VPN connection from corporate office to an Azure VNet named *hub-vnet*

Must privately access sensitive storage account from corporate office

- Disable public internet exposure

Solution: A private endpoint

- Privately connects **hub-vnet** to storage account
- Private access from corporate office
- Can also disable public access for truly private connection

Exam Tips: Azure Networking

Matthew Ulasien
Azure Training Architect

Private, Isolated Network in Azure

Required for all VMs

VMs must be in same region

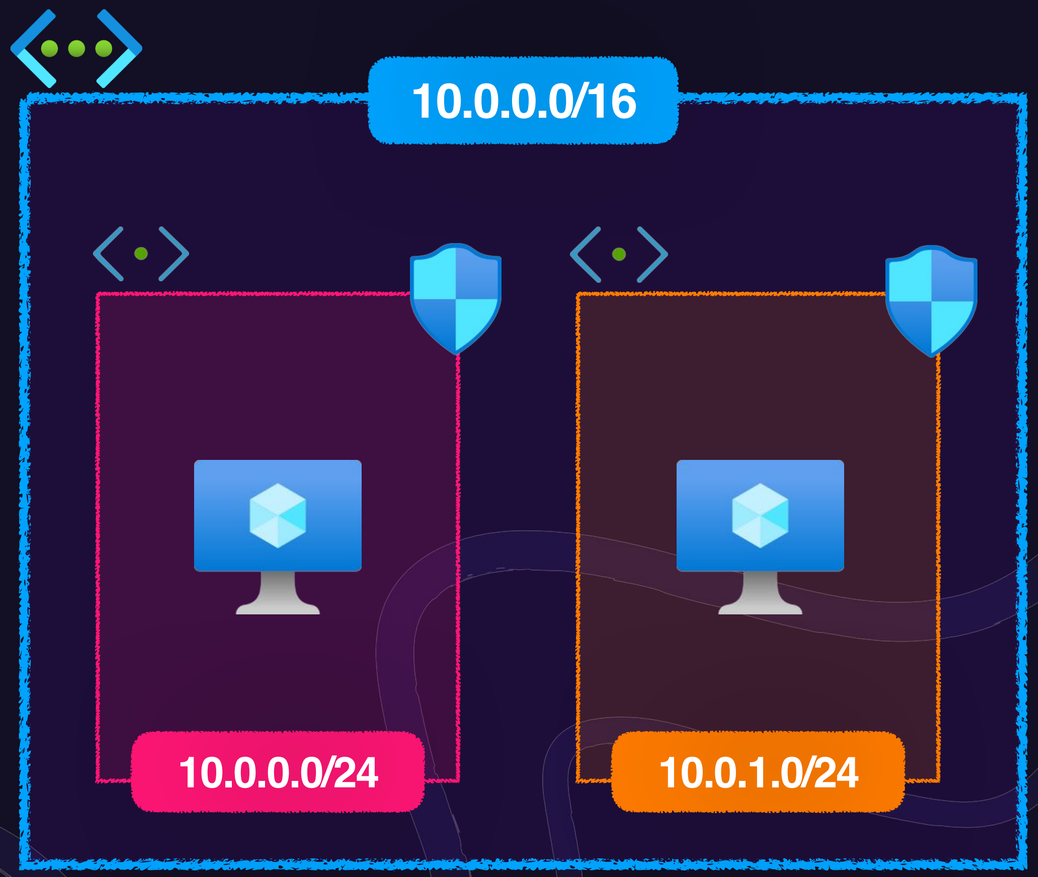
Requires Address Space and Subnet(s)

Subnet address must fit in Address Space

IP Addresses

Static vs Dynamic addresses

Private IP required, Public optional



Network Peering

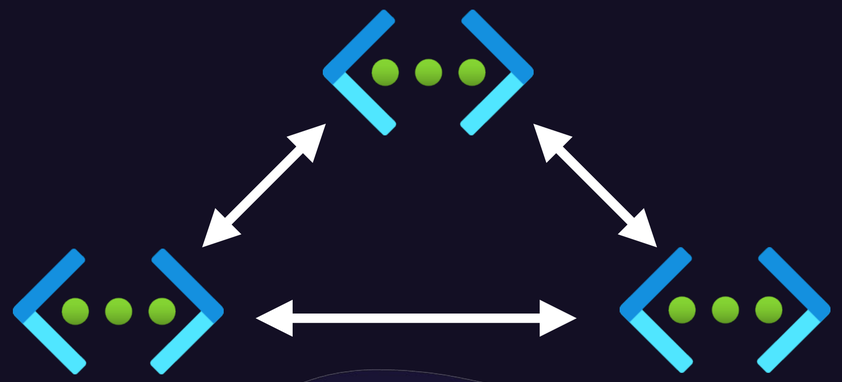
1. **Private connectivity across Azure VNets**

   Extend connectivity across multiple VNets, across Regions

2. **All traffic stays on Microsoft's private backbone**

3. **Works across subscriptions and tenants**

4. **Faster than VPN for VNet-VNet connection**



Azure DNS

1. **DNS = domain to IP translation**

   e.g. microsoft.com = 104.215.148.63

2. **Azure has both public and private DNS zones**

3. **Advantages of using Azure**

   Use existing tools

   RBAC access management

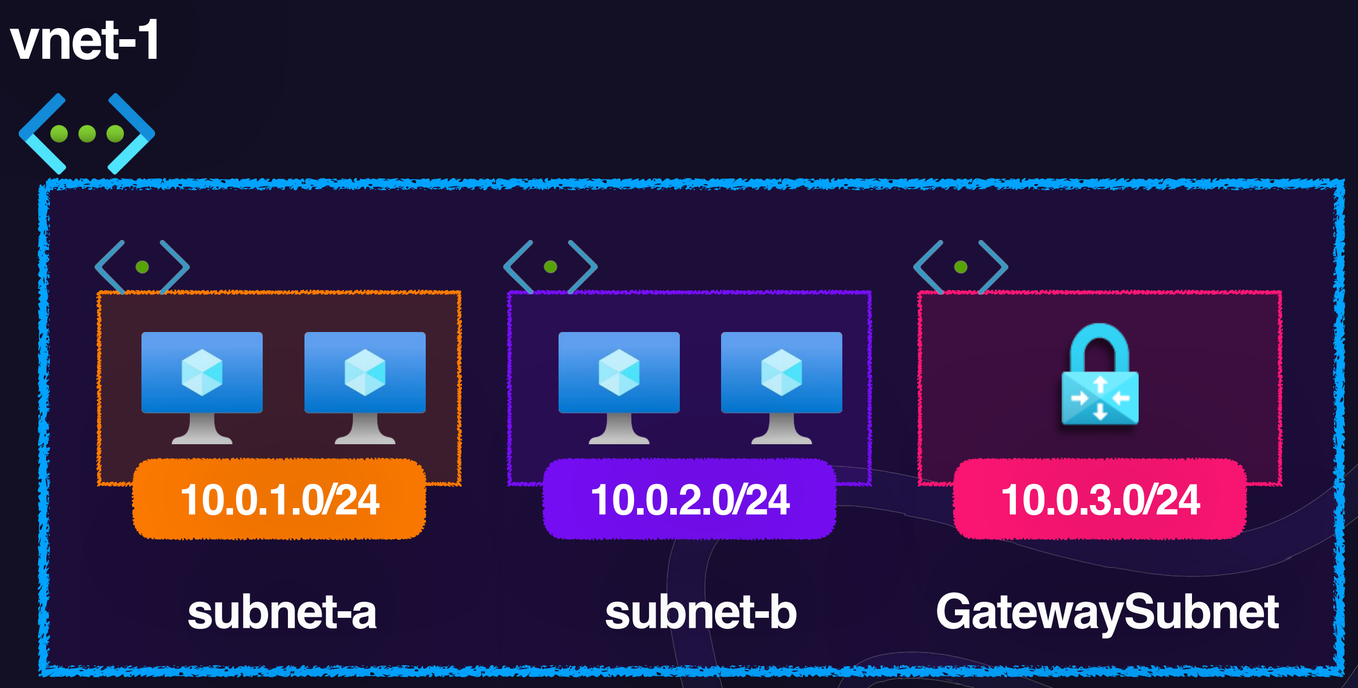
   Lock down changes

Virtual Network Gateway for all hybrid solutions

Subnet requirements

Dedicated subnet with specific name

One Network Gateway per VNet



Azure VPN

Site-to-Site vs Point-to-Site VPN

S2S = ‘Network-to-Network’

P2S = ‘Network-to-Device’

VPN Connection Method

Encrypted IPsec tunnel over public Internet

S2S VPN Components

Dedicated/named subnet

Network Gateway

Local Gateway

VPN Type: Route vs Policy based

Route based = all modern capabilities

Policy based = more backwards compatible

High Availability

Active-Standby vs Active-Active

ExpressRoute

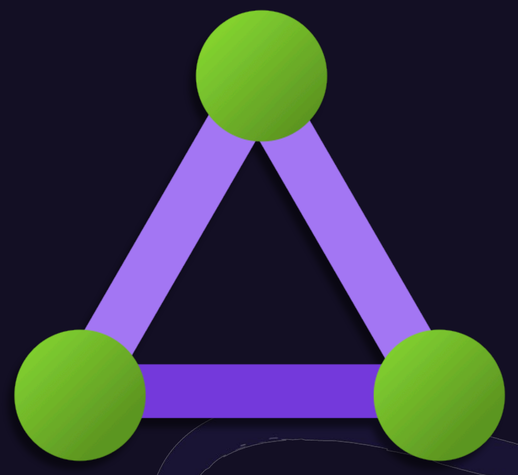
Connection format

- Private, leased lines into Microsoft's network
- Not over the public Internet
- On-premises connections only

Often partner with connectivity provider

Compared to VPN

- Faster
- Private
- More expensive
- More permanent



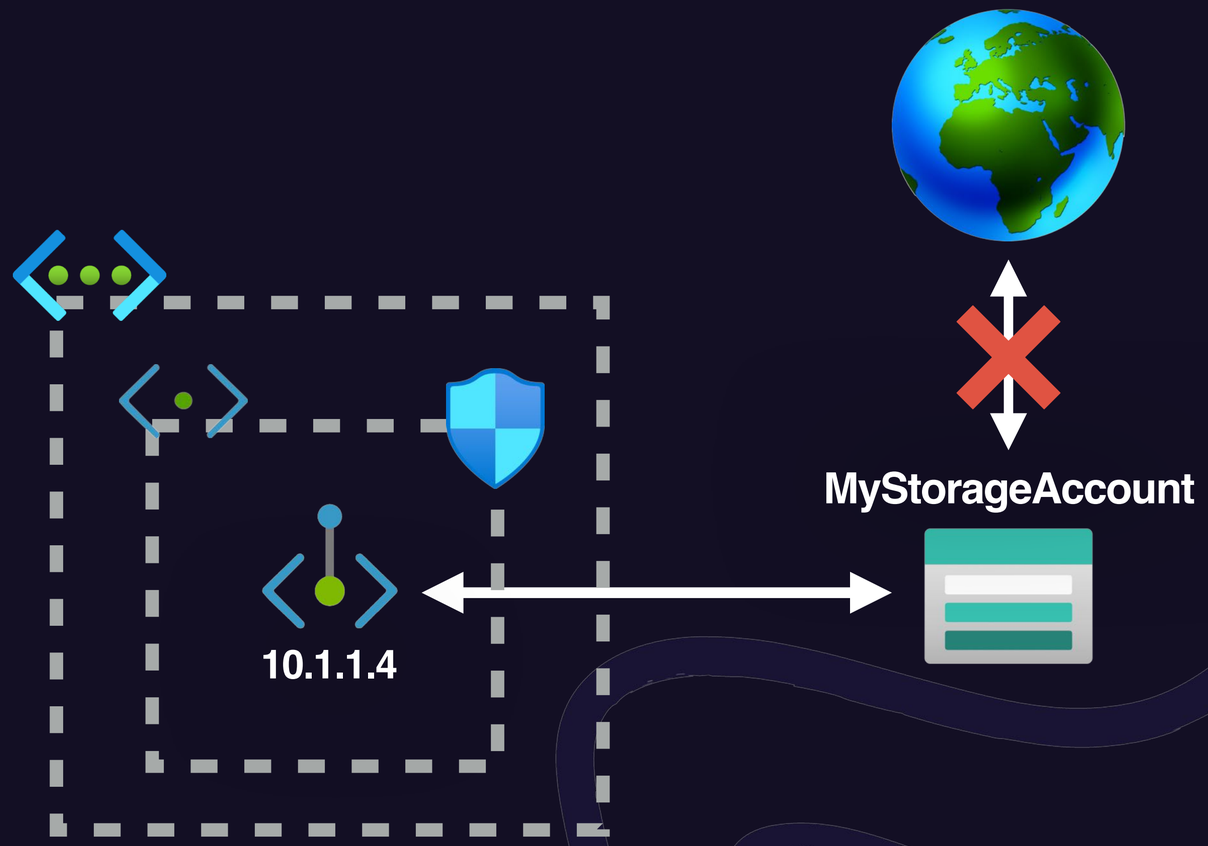
Public and Private Endpoints

Public/Private exposure for PaaS services

- Default: Public exposure for public AND VNets

Private Endpoint = Private access via VNet

- Public endpoint removed
- Private Endpoint integrated into VNet
- Shareable via connected networks



Introduction to Azure Storage

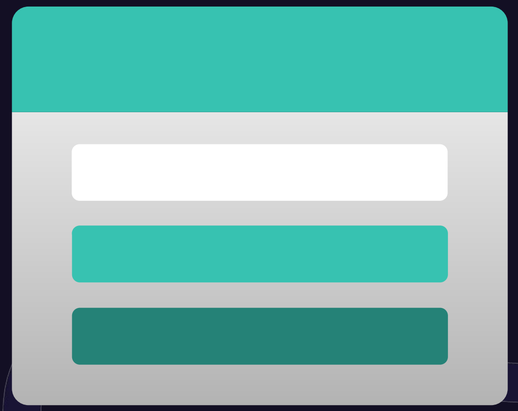
Matthew Ulasien
Azure Training Architect

Management Layer for Azure Storage Services

Configures performance, security, and access settings

Home to multiple storage services

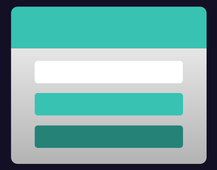
- Blob, Files, Queues, Tables, Disks, Data Lake
- Multiple instances of each storage service type



Provides unique namespace to all storage objects

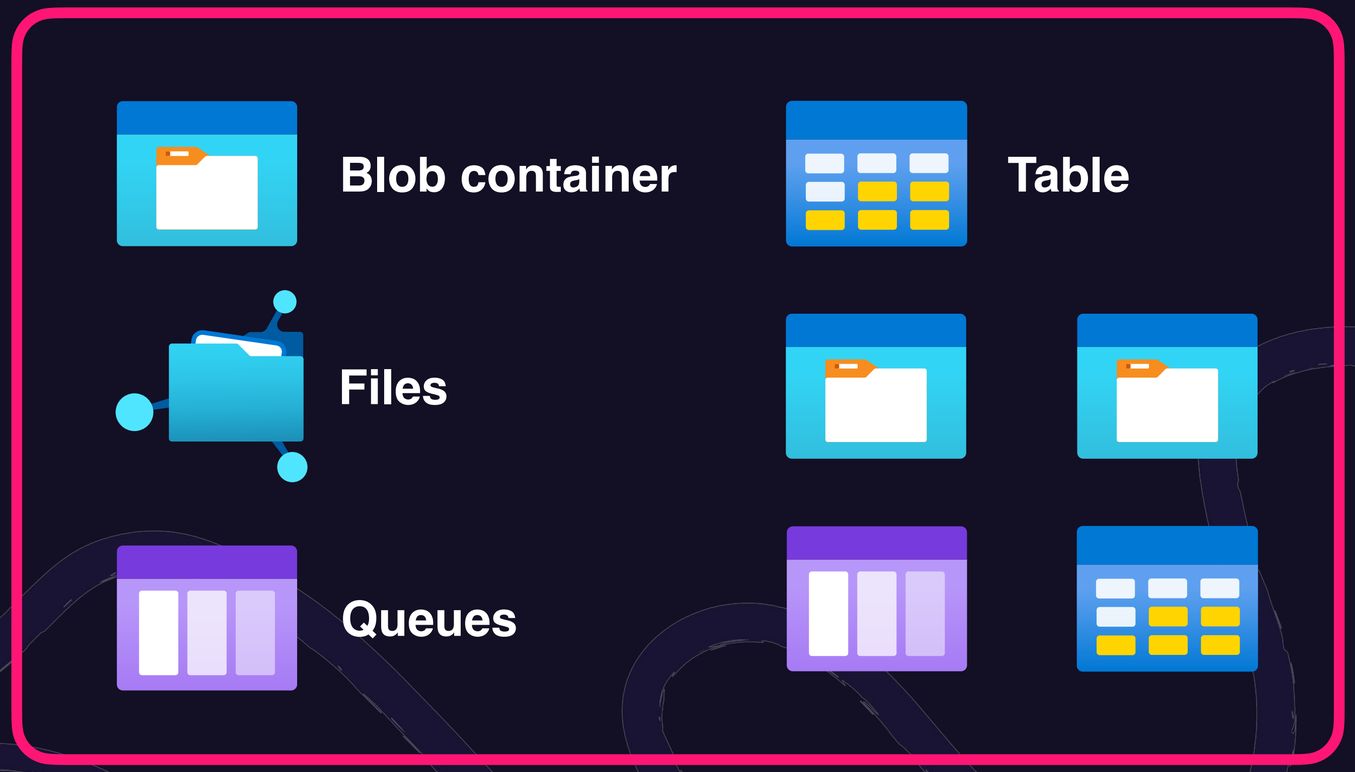
Storage Accounts and Storage Services

Management Layer



mystorageaccount

Storage Services



Storage Services

Different storage solutions within a Storage Account

Azure Blobs

Object Store

Any file type

Azure Tables

NoSQL tables

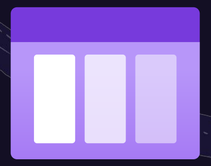
Azure Files

Managed file share (file server)

Azure Disks

Managed VM Disks

Not managed in Storage Account



Azure Queues

Messaging store between application components

Unique Namespace for Storage Account

Account name must be globally unique

- Namespace given for all endpoints/storage services
- Lowercase and numbers only
- Every storage service has its own address

Blob Storage	https://<storage-account-name>.blob.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net

Azure Blobs

Matthew Ulasien
Azure Training Architect

What Is Blob Storage?

Unstructured Data Storage

Blob = Binary Large Object

Which is pretty much ANY file

Can store massive amounts of data

Petabytes of storage

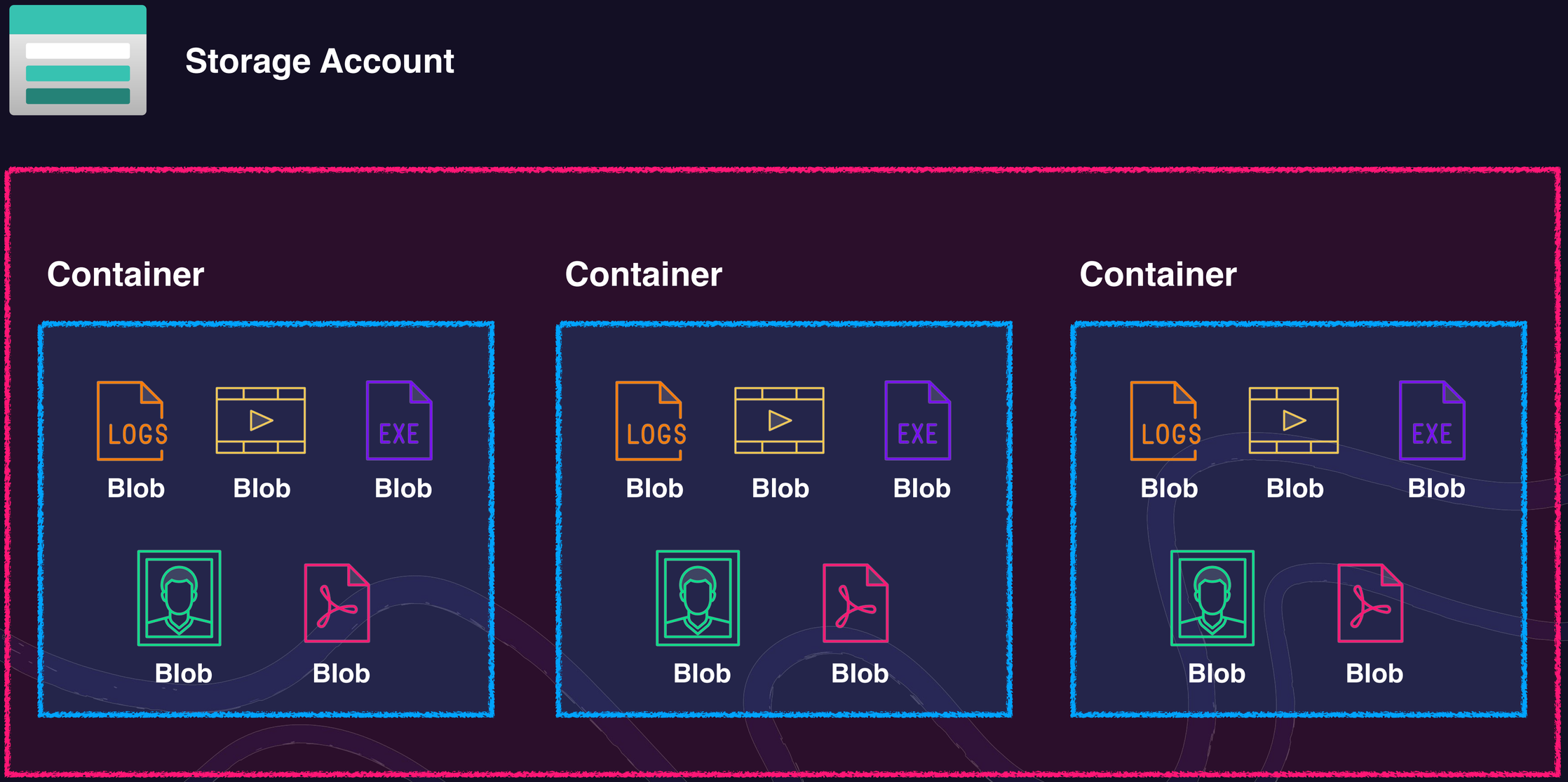
Blobs stored in containers

Multiple storage tiers to balance performance/cost

Don’t need to pre-provision space. Charged by actual space used.

Azure Blobs

Blob Storage Layers



Web Access for Blobs

Each blob has a web address

Blobs can be private or public

Private by default

Address format

https://<storage-account>.blob.core.windows.net/<container>/<folder>(optional)/<blob>

https://mystorageaccount.blob.core.windows.net/images/funnycat.jpg

Storage Account

Container

Blob

Blob Types

1. **Block**

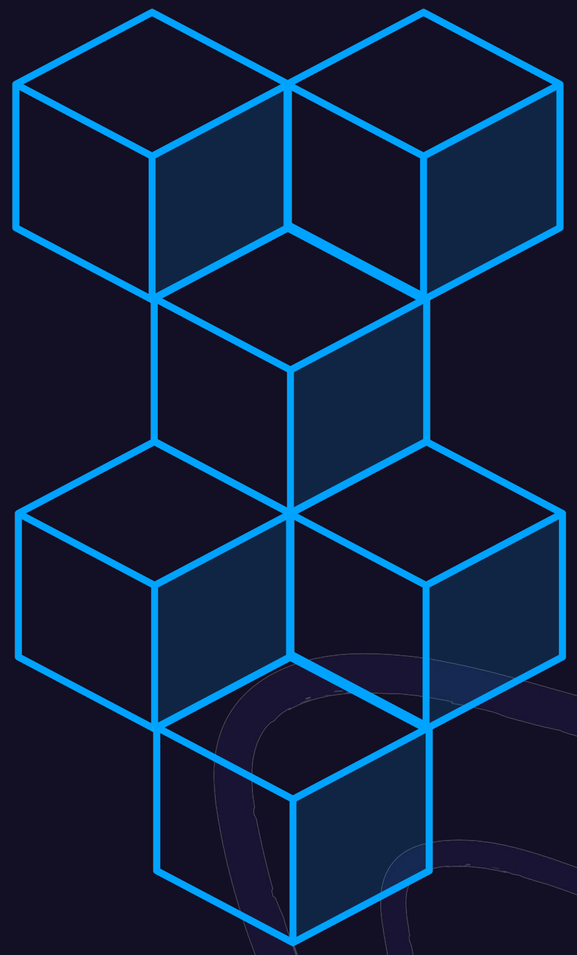
   Store text and binary data up to about 4 TB. Made up of individually managed blocks of data.

2. **Append**

   Block blobs that are optimized for append operations. Works well for logging where data is constantly appended.

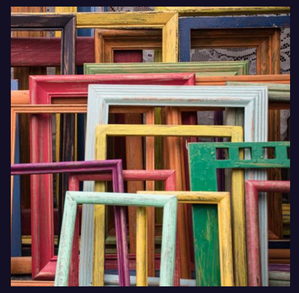
3. **Page**

   Store files up to 8TB. Any part of the file could be accessed at any time, for example a virtual hard drive.



Azure Blobs

Blob Storage Use Cases

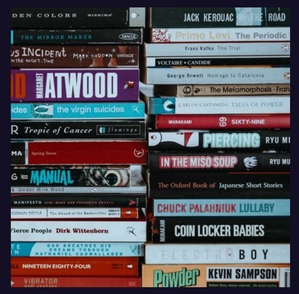


Images for public website

Single image storage location for all sizes and formats

Log Files

Write to log files regardless of size and frequency.

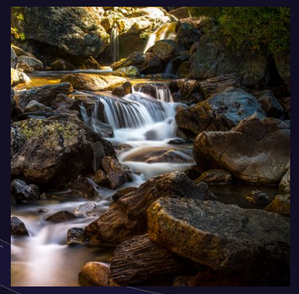


File storage

Though not a file server, can still act as file storage location

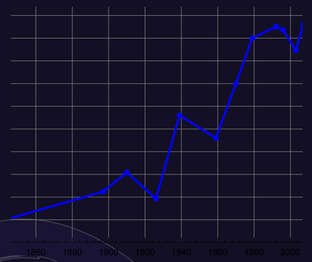
Data Store

Store any kind of data at scale, such as for archiving, backup, restore and disaster recovery.



Streaming

Stream audio and video directly from your blob storage.



Data Analysis

Data storage for Azure or other data analysis products

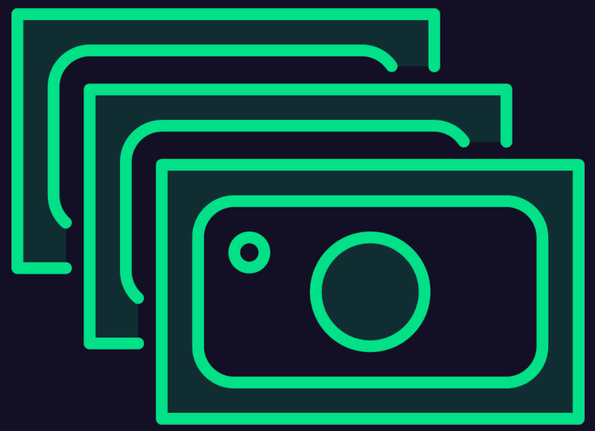
Blob Storage Tiers

Matthew Ulasien
Azure Training Architect

The Problem To Solve

Expanding Storage Needs = Higher Costs

- Not all stored data needs frequent, instant access
- Data accessed less frequently = wasted money



Solution: Optimize costs with tiered storage based on access needs

Storage Tiers

Online

Hot

Frequently accessed data

Cool

Less frequently accessed

Cold

Even less frequently accessed

Offline

Archive

Rarely accessed, if ever

Blob Storage Tiers

Balance Storage Costs With Usage/Retention Costs

1. **Cheaper storage tiers have higher minimum retention + higher usage costs**
   Minimum retention = How long data must exist before deletion

2. **Accessing cheaper storage tier data has extra cost**
   Frequently accessed data needs to be hot tier

Hot	Cool	Cold	Archive
Frequently accessed data	30 days	90 days	180 days

Archive Storage Tier

Only NOT instantly accessible option

1. **Offline data for VERY rare access needs**

2. **Archive data must be ‘rehydrated’**
   - Must request data to be brought back online
   - Rehydration time measured in **hours**
   - Rehydration request has additional cost

3. **Archive scenarios:**
   - Long-term compliance archiving, Legal hold data

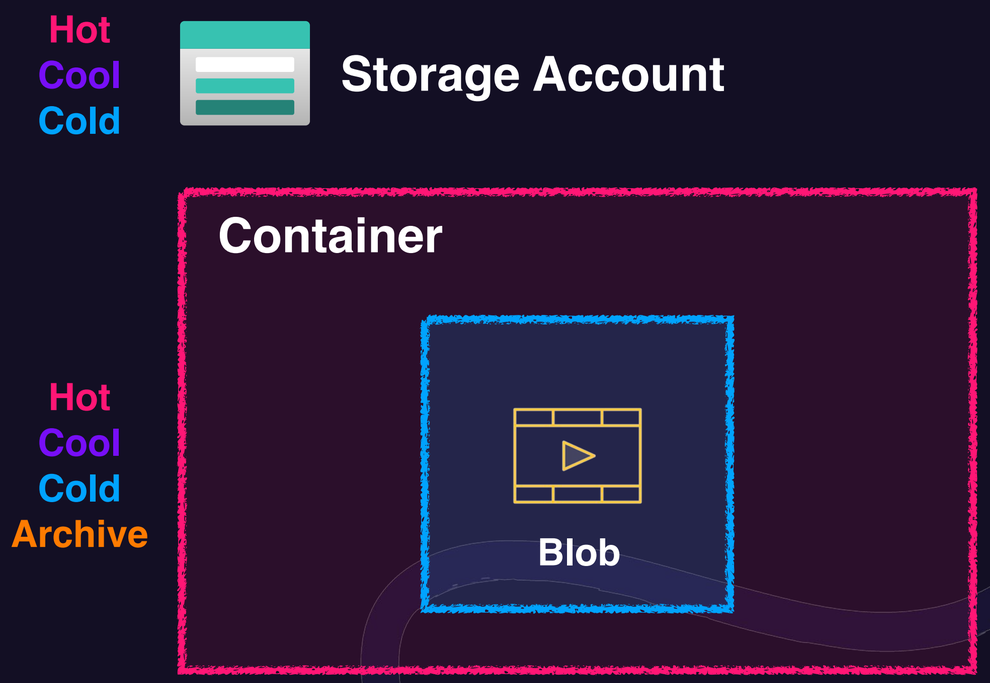
Configuring Storage Tiers

Storage Account vs blob-level configuration

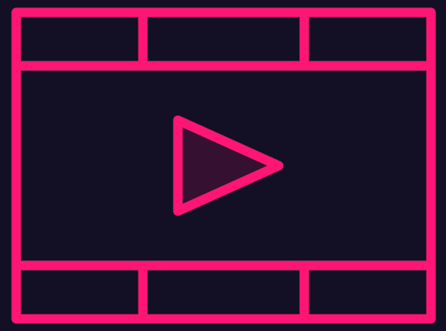
- Account-level: Default tier for new objects
  - Hot/Cool/Cold (not Archive)
- Blob-level
  - All levels

Existing blobs can change tiers

- Example: Hot —> Cold



Scenarios

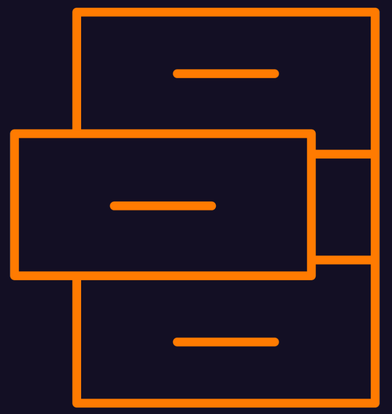


Hot

Real-time analytics data
Website images/videos

Cool/Cold

Short term backups
Seasonal data



Archive

Medical records
Historical Data

Demo: Create a Storage Account

Matthew Ulasien
Azure Training Architect

Demo

Create a Storage Account

- Jump into uploading blobs in next lesson

Pay attention to:

- Naming requirements
- Default storage tier options
- Redundancy and premium options (will be covered later)

Demo: Upload Files to a Blob Container

Matthew Ulasien
Azure Training Architect

Demo

Create container

Upload files (objects) to container

Browse files with Storage Explorer

Explore:

- Object URL
- Setting storage tiers
- Access methods

Summing It Up

Creating a Blob Container

- Access methods
- Unique URL
- Setting storage tiers

Disks

Matthew Ulasien
Azure Training Architect

Storage Accounts

Managed Disks for VMs

VM Disks backed by Azure Storage

Storage account management abstracted away

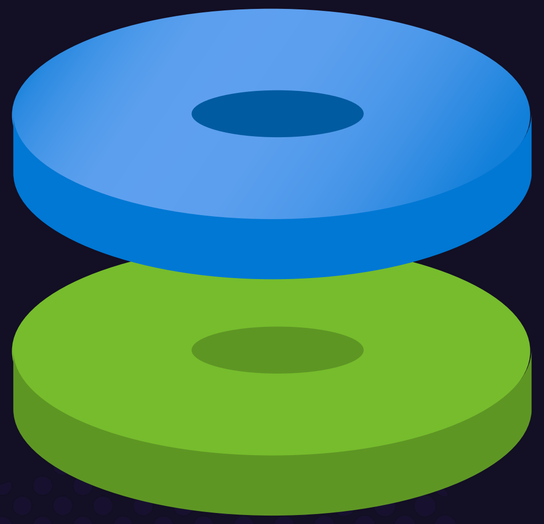
No Storage Account interaction

Provision your disk, and Azure handles the rest

‘Unmanaged’ disks are being removed

Import .vhd files from on-premises

Import on-premises disks into Azure



Disk Types

HDD

Spinning hard drive. Low cost and suitable for backups.

Standard SSD

Standard for production. Higher reliability, scalability and lower latency over HDD.

Premium SSD/v2

Super fast and high performance. Very low latency. Use for critical workloads.

Premium SSDv2 up to 64TB

Ultra Disk

For the most demanding, data-intensive workloads. Disks up to 64TB.

Disks Comparison

	Ultra disk	Premium SSD v2	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance-sensitive workloads that consistently require low latency and high IOPS and throughput	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 GiB	65,536 GiB	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	4,000 MB/s	1,200 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	160,000	80,000	20,000	6,000	2,000, 3,000*
Usable as OS Disk?	No	No	Yes	Yes	Yes

Demo

Create a Disk

- Not using storage account interface

Attach Disk to a VM

- Disk and VM must be in same region

Azure Files

Matthew Ulasien
Azure Training Architect

The Problem to Solve

On-Premises Storage

Issues

1. **Constraints**
   You only have a limited amount of storage.

2. **Backups**
   Time and resources spent on maintaining backups.

3. **Security**
   It can be hard to keep all data secure at all times. Specialist assistance often needed.

4. **File Sharing**
   Can be difficult to share files across teams and organizations.

What is Azure Files?

Fully Managed Cloud-based file share/server solution

1. **SMB and NFS Protocols**
   Windows/Linux file shares

2. **Available on Windows/Mac/Linux**

3. **Flexible Deployments**
   Cloud-only or synced to on-premises file servers with **Azure File Sync**
   Fast access near your users, in multiple locations

Azure Files

Benefits

1 **Replace/Synchronize File Servers**

Maintain application compatibility

2 **Managed**

You don’t have to worry about hardware or operating system.

3 **Scripting and Tooling**

Use existing file server management tools

PowerShell cmdlets, Azure CLI

Use familiar file system APIs

Azure Files

Scenarios

Hybrid

Supplement or replace your existing on-premises file storage solution.

Lift and Shift

Move your existing file storage and related services to Azure.

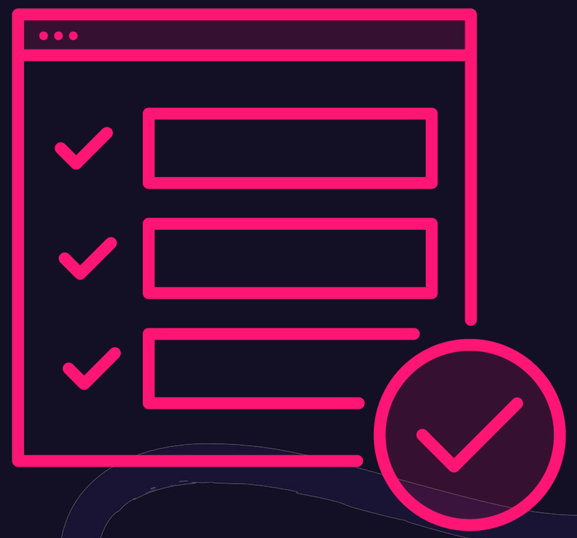
Tables and Queues

Matthew Ulasien
Azure Training Architect

Exam Scope

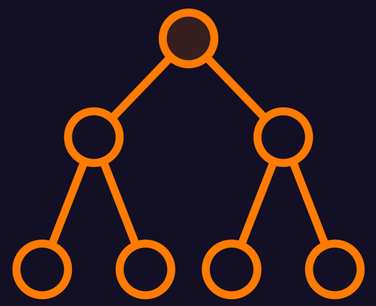
Not currently part of AZ-900 exam

- However, still worth covering since part of Azure Storage
- Brief Overviews



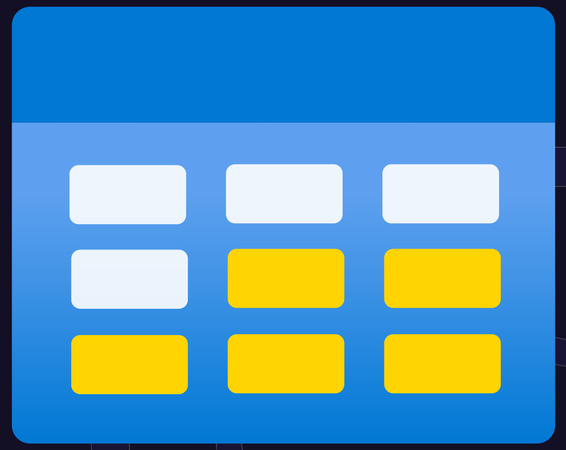
Azure Tables

NoSQL Storage for structured, scalable data



1. **Large volumes of NoSQL/non-relational data**
   NoSQL = more flexible data structure than relational format
   Relational = columns/rows

2. **Hybrid and multi-cloud setups**
   Can be integrated with Azure/non-Azure solutions
   Cost-effective, lightweight database solution

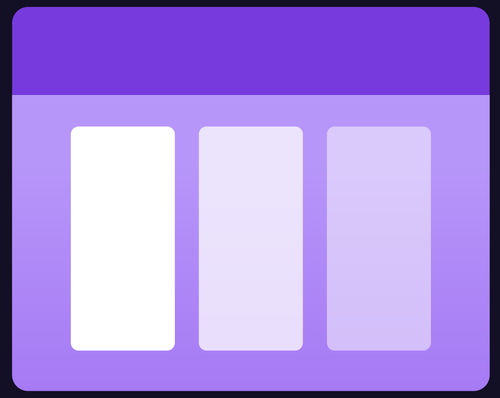


3. **In transition to migrate to CosmosDB**
   Azure Storage product remains, but CosmosDB version has better capabilities

Azure Queues

Message storage for asynchronous task processing

1. **Store large volumes of messages**
   - Messages = data sent from/to different applications
   - Deliver/retrieve over HTTP/HTTPS
   - Example: Order processing system
2. **Asynchronous Processing**
   - Application components aren’t directly linked
   - Can allow backlog of messages to be processed later

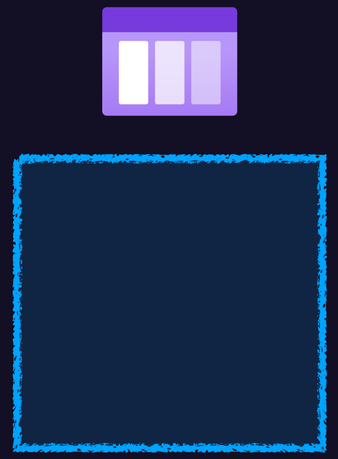


Scenario: Azure Queues

Order Processing Pipeline

Order placed

Order details



Sent to Azure Queues

Azure Function takes message to fulfillment center

Storage Redundancy

Matthew Ulasien
Azure Training Architect

Importance of Data Redundancy

Accidents Happen!

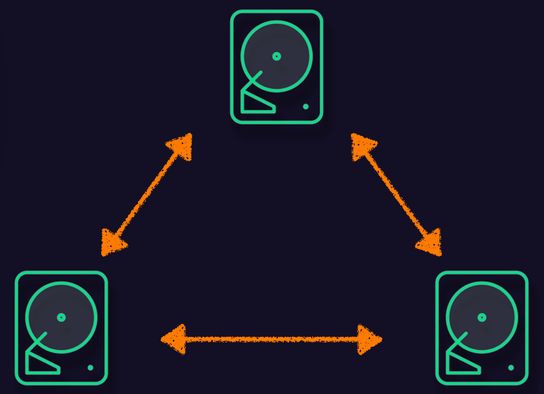
Hardware Failure

Zone/Regional Outage

Data redundancy protects against unplanned failures.

Redundancy: Multiple, Replicated Copies of Data

If one copy fails/is inaccessible, data is still available.



Azure Storage always creates multiple copies of your data:

- Automatic
- **Minimum** of three copies
- Invisible to end user

Multiple Redundancy Options

- Different location scopes
  - **Single zone**, **multiple zones**, **multiple regions**
- Higher availability = higher cost

Locally-redundant storage (LRS):
Lowest-cost option with basic protection against server rack and drive failures. Recommended for non-critical scenarios.

Geo-redundant storage (GRS):
Intermediate option with failover capabilities in a secondary region. Recommended for backup scenarios.

Zone-redundant storage (ZRS):
Intermediate option with protection against datacenter-level failures. Recommended for high availability scenarios.

Geo-zone-redundant storage (GZRS):
Optimal data protection solution that includes the offerings of both GRS and ZRS. Recommended for critical data scenarios.

Redundancy Options at a Glance

Single Region

Locally Redundant Storage
(LRS)

Zone-Redundant Storage
(ZRS)

Multi-Region

Geo-Redundant Storage
(GRS)

Geo-Zone-Redundant Storage
(GZRS)

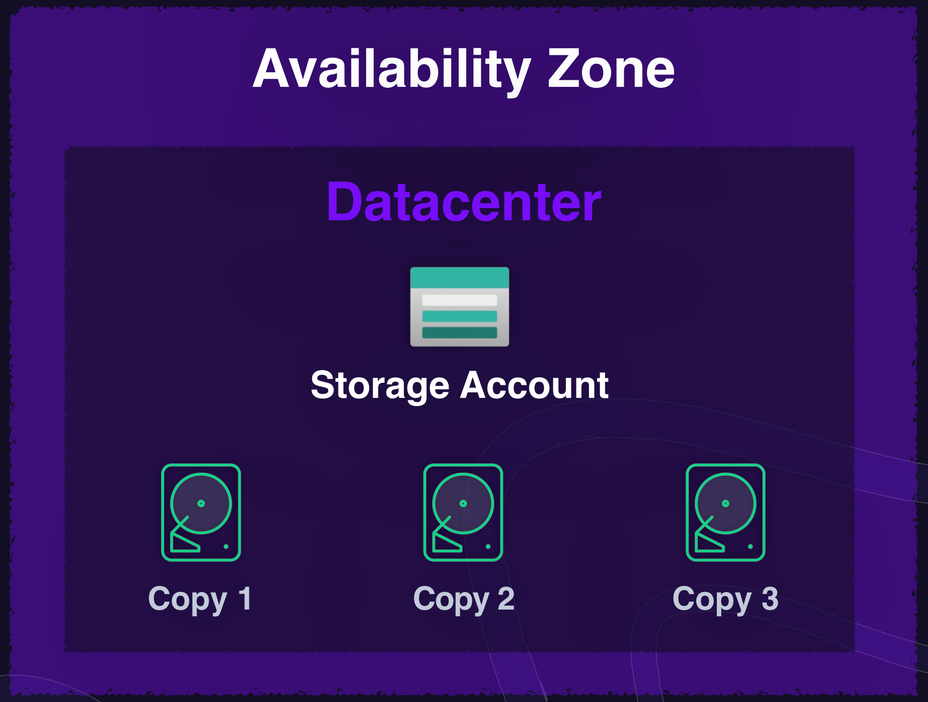
All options include:

- **Three copies** in primary region
- **Three copies** in secondary region (multi-region options)

Locally Redundant Storage (LRS)

Three copies in single location (datacenter/zone)

1. Lowest-cost option
2. Protect against single disk failure
3. Does not protect against zone or regional outage



Zone-Redundant Storage (ZRS)

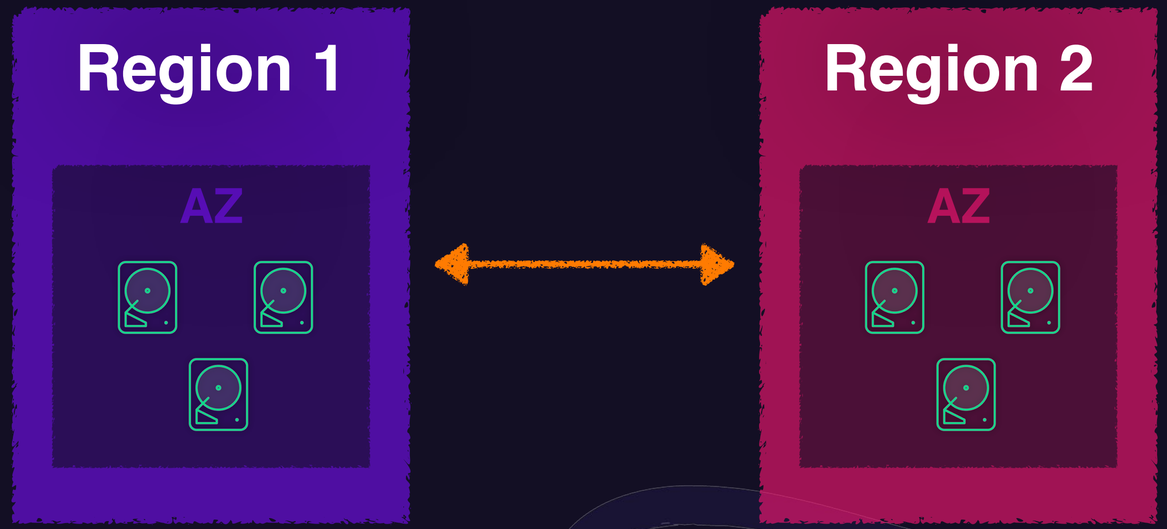
Three copies across three availability zones

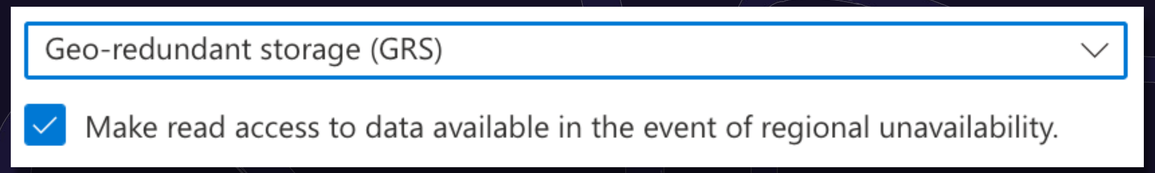
1. One copy in each zone
2. Protect against zone outage but not regional outage

Geo-Redundant Storage (GRS)

Three copies in two different regions

1. Three copies in primary regional physical location (LRS)
2. Three copies in secondary (paired) region physical location (LRS)
3. Protect against primary region failure but no primary region zone redundancy
4. Can configure read access from secondary region for high availability

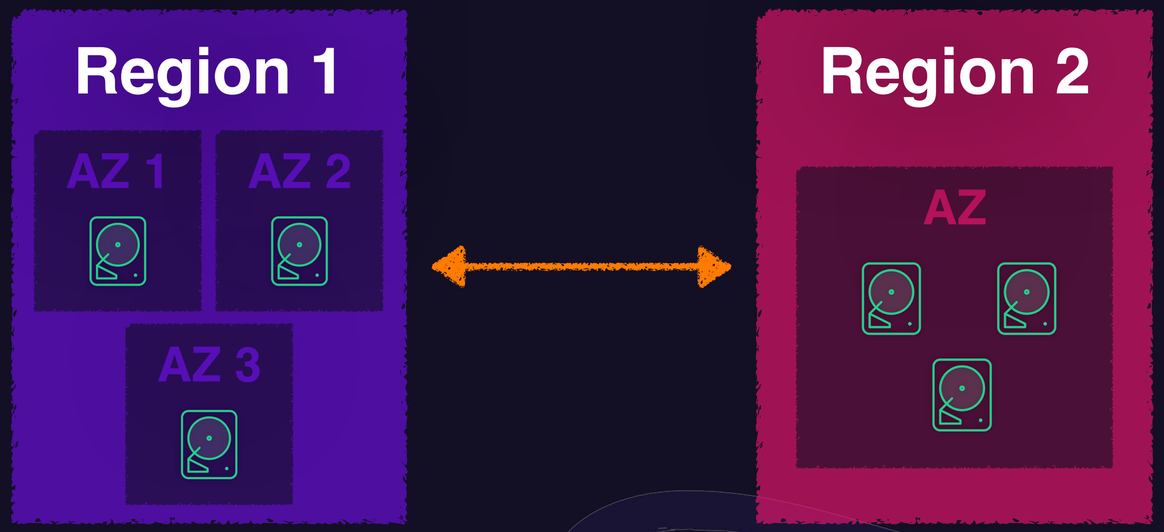


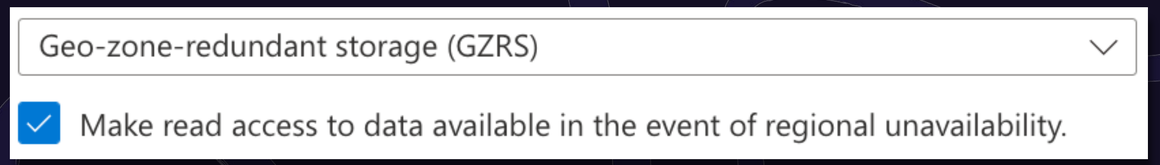


Geo-Zone-Redundant Storage (GZRS)

Maximum redundancy!

1. Copy across three availability zones in primary region (ZRS)
2. Three copies in secondary region physical location/zone (LRS)
3. Protect against primary region failure AND primary region zone failure
4. Can also configure read access from secondary region for high availability





Storage Redundancy

Azure Storage automatically replicates data for redundancy

- Three copies in single region
- Six copies across two paired regions
  - Three in each region

Redundancy options vary by availability and cost

- Single zone
- Multiple zones in a single region
- Across regions
  - Single/multi-zone in primary region

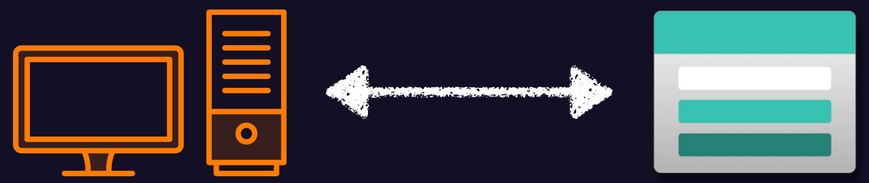
Moving Data in Azure Storage

Matthew Ulasien
Azure Training Architect

Concept: Moving Data Into and out of Azure Storage

Different solutions based on:

- Transfer frequency (occasional/continuous)
- Data size
- Network bandwidth



AZ-900 focus for smaller, occasional transfers:

AzCopy

Azure Storage Explorer

Azure File Sync

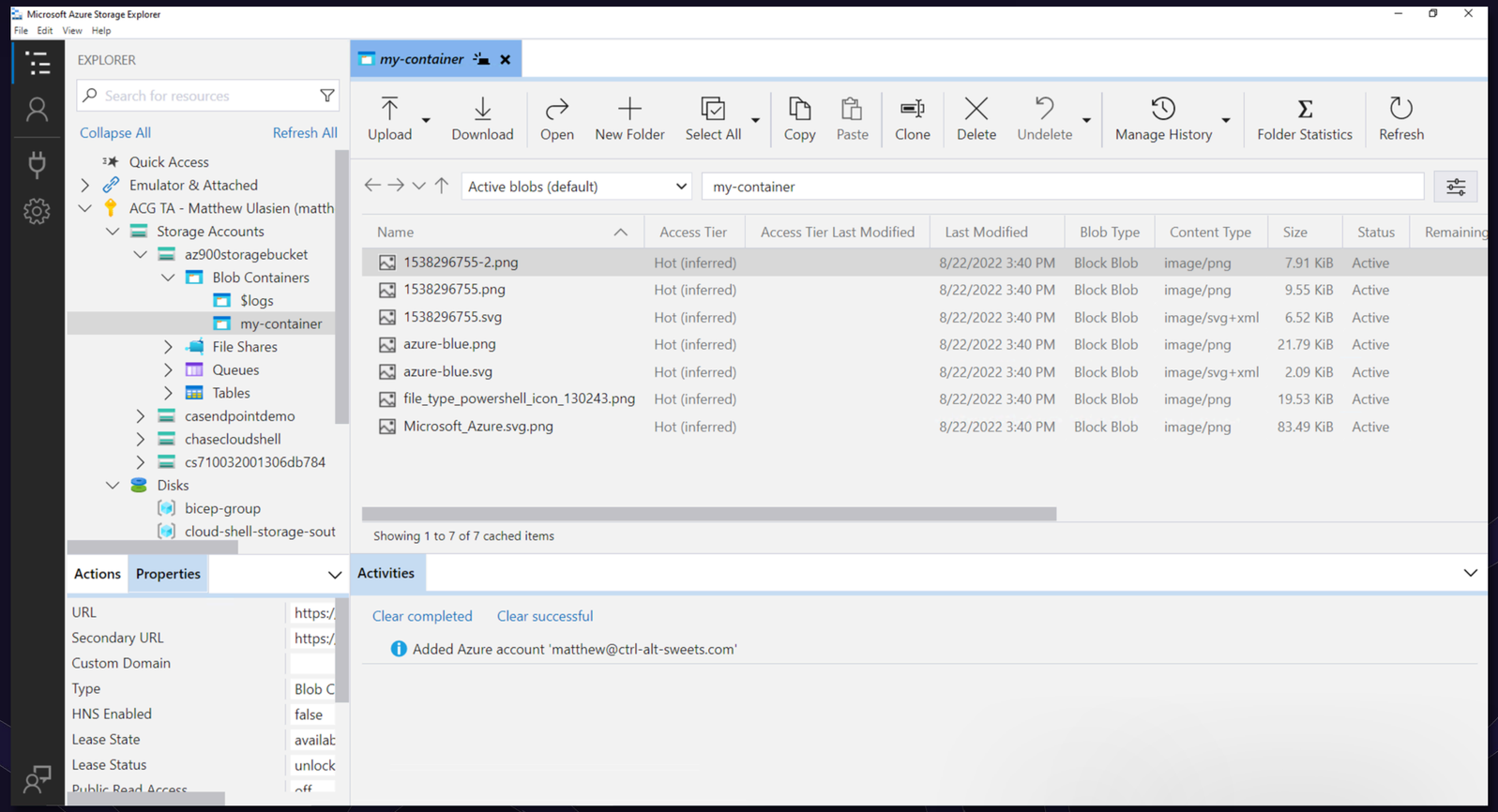
Command-Line Utility

1. Transfer blobs and Azure Files
2. Useful for scripting data transfers

```
azcopy cp “funny-llamas.mp4” "https://mystorageaccount.blob.core.windows.net/my-container"
```

Graphical User Interface (GUI) Interaction

1. **Downloaded application**
2. **User-friendly graphical interface**
   - Drag-and-drop interaction
3. **Move all storage account formats**



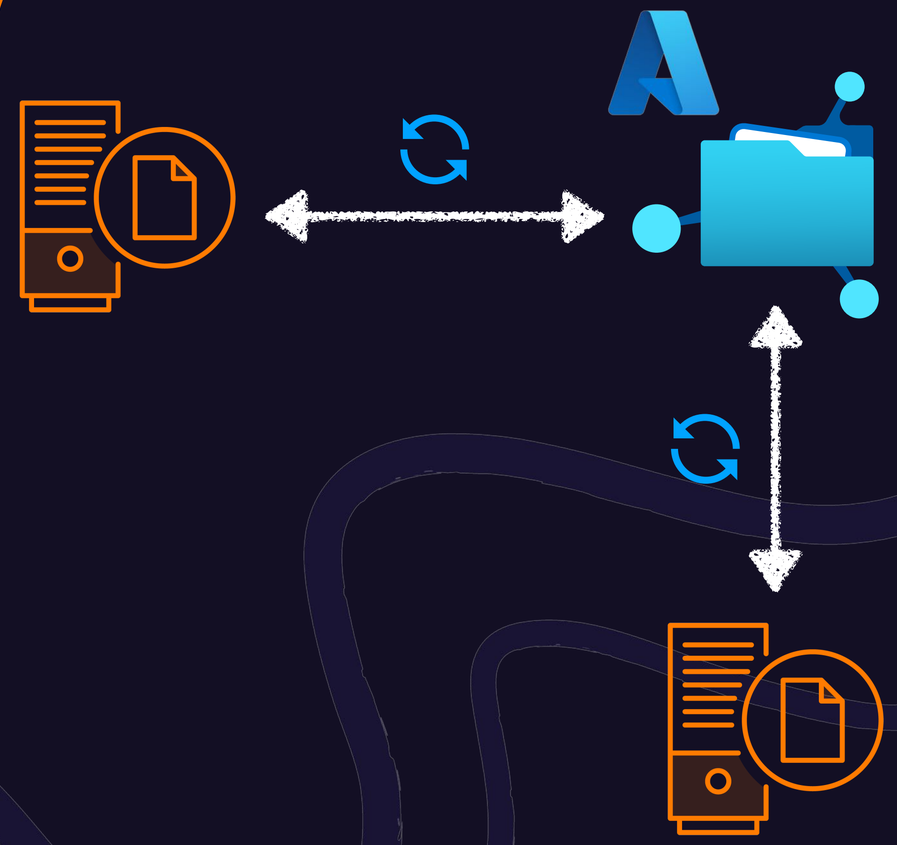
- from the *Azure Storage Explorer UI*

Synchronize Azure Files with On-Premises File Servers

Local file server performance + cloud availability

Use cases:

- Back up local file server
- Synchronize files between **multiple** on-premises locations
- Remote users access Azure Files
- Transition to only Azure Files for file server



Demo: Azure Storage Explorer and AzCopy

Matthew Ulasien
Azure Training Architect

Demo

Azure Storage Explorer

- Upload blob files
- Create file store

AzCopy:

- Use Cloud Shell
  - Pre-installed/authenticated
- Upload and work with blob files in container

Additional Migration Options

Matthew Ulasien
Azure Training Architect

Two More Migration Solutions

Azure Data Box

Azure Migrate

Azure Data Box

Scenario: Transfer LOTS of data and/or limited bandwidth

- **Lots** = Too much to transfer over the internet
- Relative to available network bandwidth

Offline data transfer to/from Azure

Copy data to physical data storage device (Data Box)

- Encrypted
- Rugged

Ship Data Box to/from Azure

- **To Azure:** Data Box data transferred to storage account
- **From Azure:** Data Box delivered to on-premises location for on-site transfer

Data Box Use Cases

Initial bulk data migration

Disaster recovery

- Restore Azure backup to on-premises location

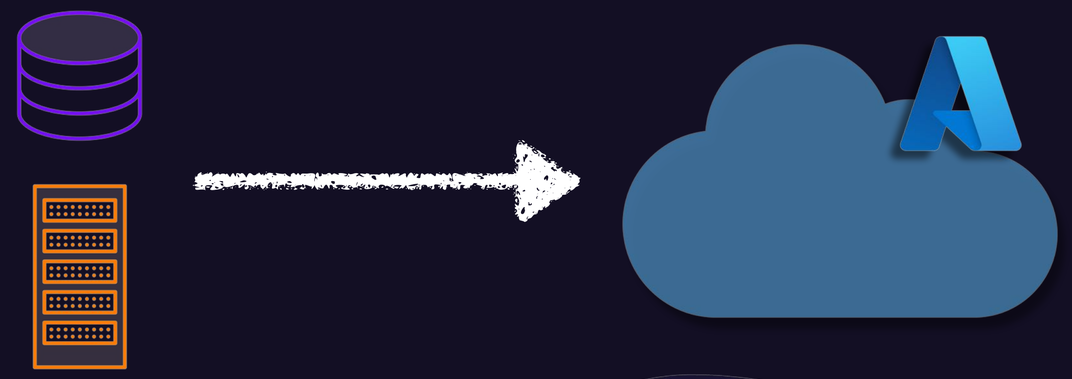
Security requirements

- Sensitive data that cannot be sent over the internet

Azure Migrate

Migrate non-Azure resources into Azure

- Servers
- Databases
- Applications



Includes, but not limited to, migration to storage accounts

Additional Migration Options

Azure Migrate Scenario: Migrate Datacenter to Azure

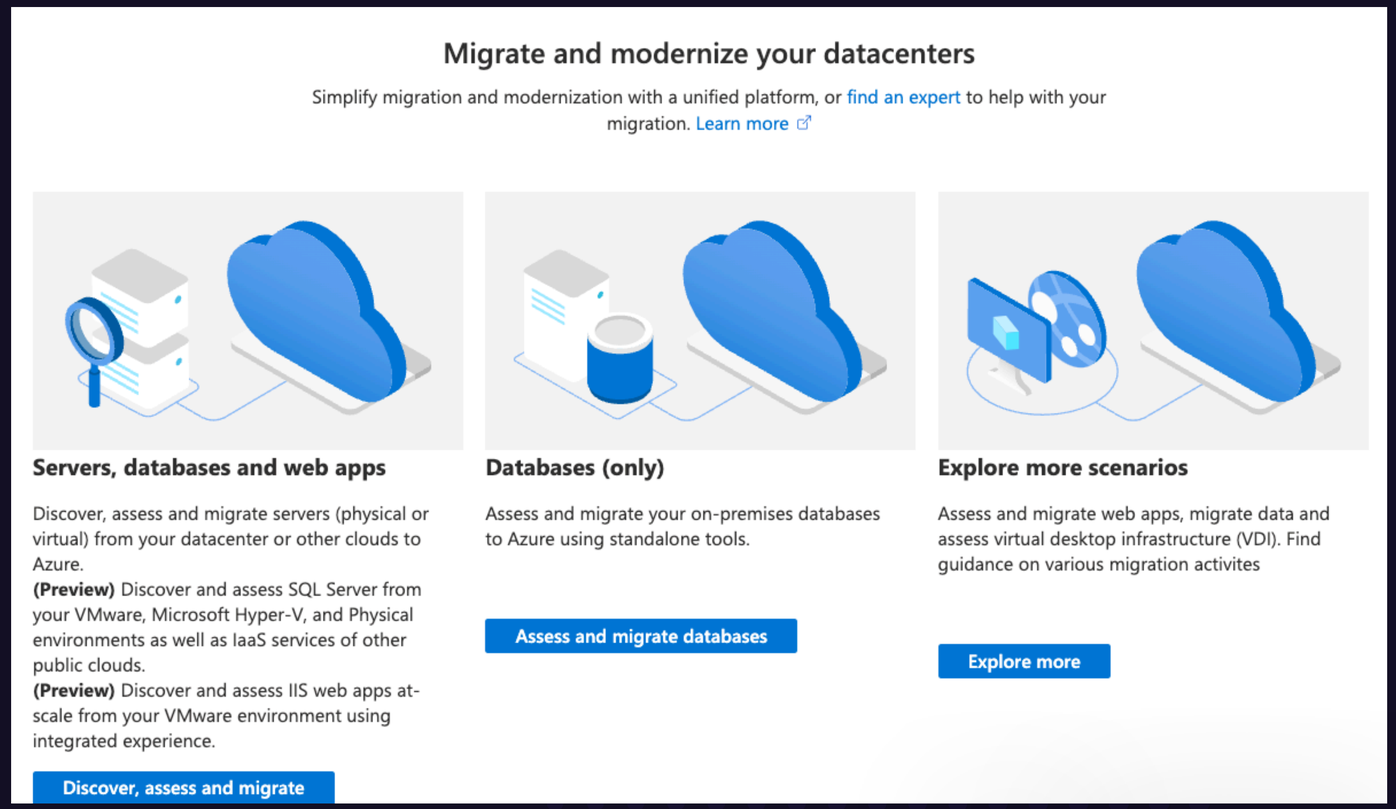
Discover dependent resources to migrate.

Migrate VMs.

Migrate databases to managed database services (e.g., Azure SQL).

Migrate on-premises applications and dependencies.

Migrate bulk data with Data Box.



- from the *Azure Migrate Dashboard*

Premium Performance Options

Matthew Ulasien
Azure Training Architect

Premium Performance Options for Low-Latency Requirements

Stored on SSDs

Key considerations:

- Available storage types for each performance option
- Redundancy options
  - Trade more performance for less redundancy
- All premium options have a higher cost

Storage Account Performance Options

Standard

Standard general-purpose v2

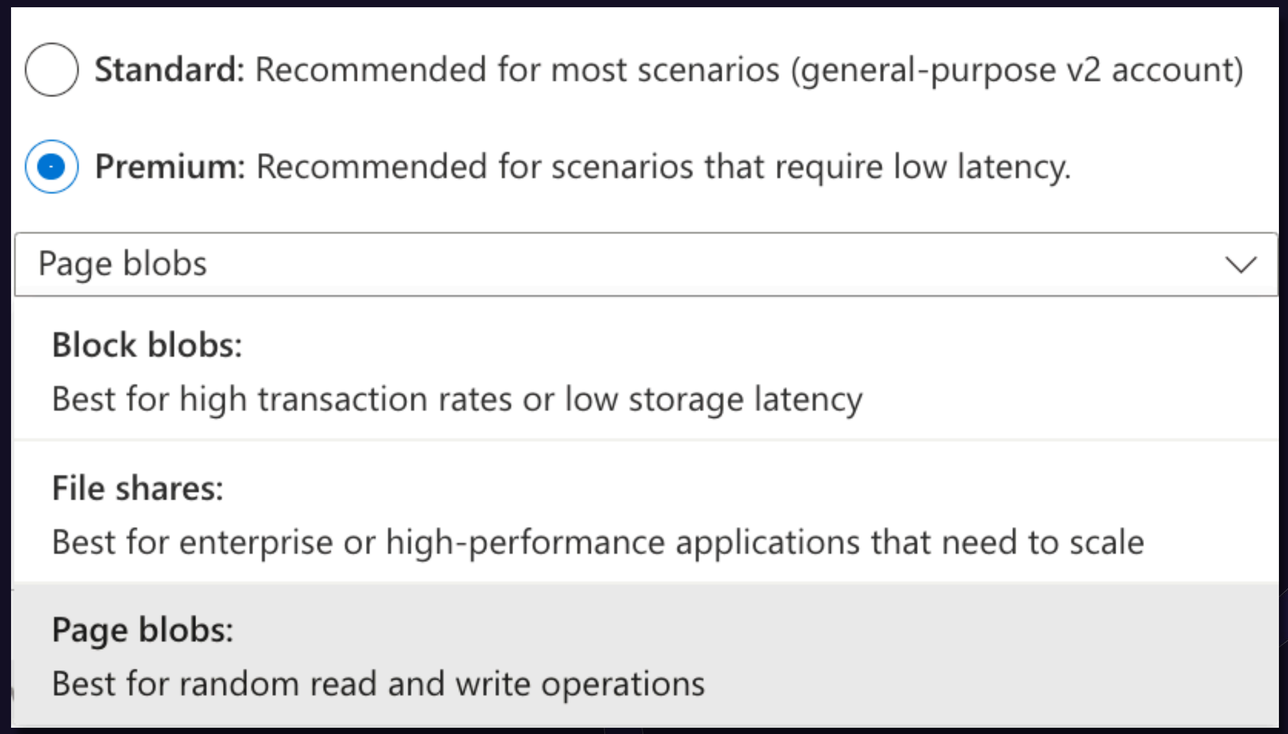
- The default — supports all storage types
- All redundancy options

Premium

Premium block blobs

Premium page blobs

Premium file shares



Premium Block Blobs

Supported Storage Type

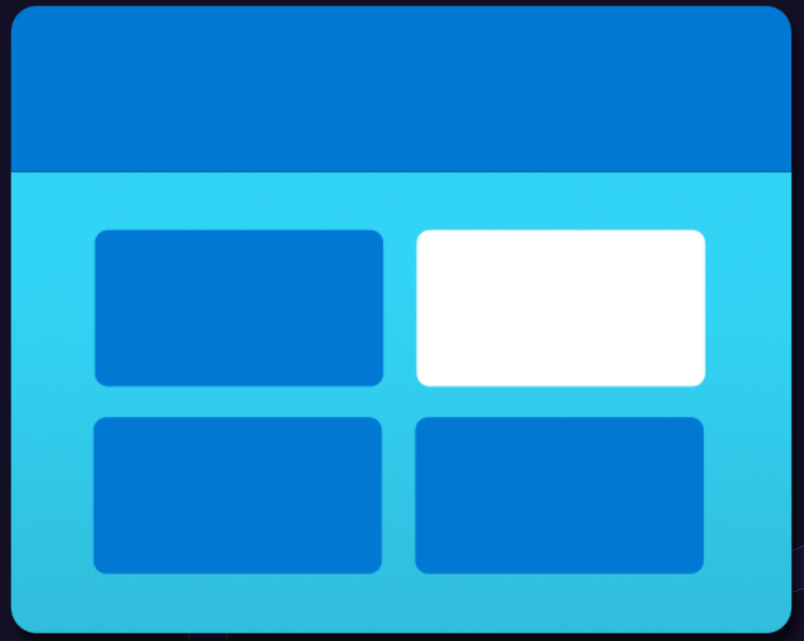
Blob Storage

Ideal for low-latency blob storage workloads

- AI applications, IoT analytics

Redundancy

LRS/ZRS only



Premium Page Blobs

Supported Storage Type

Page blobs

- Unmanaged virtual disk (currently being retired)
- Standalone API access

Redundancy

LRS only (single zone)

Premium File Shares

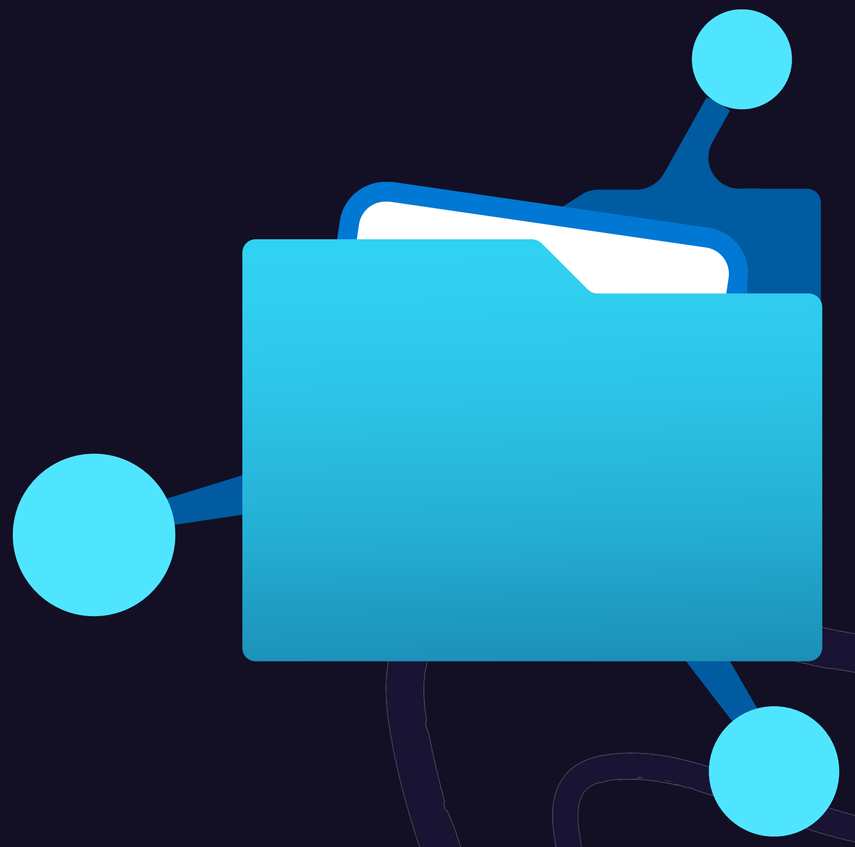
Supported Storage Type

Azure Files

Ideal for high-performance enterprise (file server) applications

Supports both Server Message Block (SMB) and Network File System (NFS) file shares

- Windows/Linux file shares



Redundancy

LRS/ZRS only

Premium Storage Summary

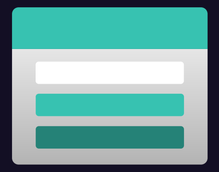
Type of Storage Account	Supported Storage Services	Redundancy Options
Premium block blobs	Block blob Storage	LRS/ZRS
Premium page blobs	Page blobs only (IaaS disks)	LRS
Premium file shares	Azure Files	LRS/ZRS

Exam Tips: Azure Storage

Matthew Ulasien
Azure Training Architect

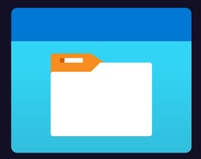
Storage Accounts and Services

Management Layer



mystorageaccount ← Globally unique name

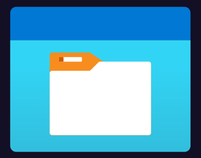
Storage Services

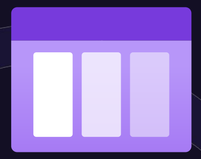


Blob container

Table

Files





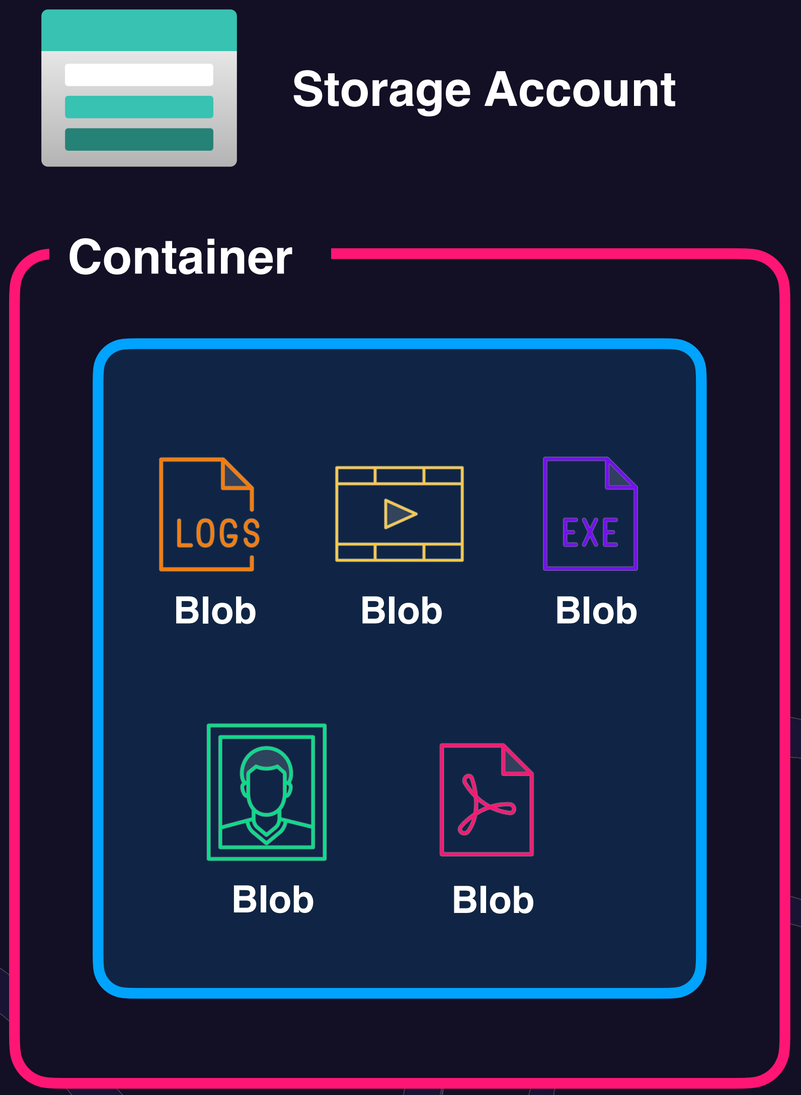
Queues

Azure Blobs

1. **Unstructured data store**
   Any file type

2. **Blobs stored in containers**

3. **Blob types**
   Block - ‘loose files’
   Append - Added-on-to files (logs)
   Page - virtual hard drive



Blob Storage Tiers

Cheaper storage with restrictions

1. **Hot/Cool/Cold/Archive**

   Each tier down cheaper
   Longer retention periods
   Higher access costs

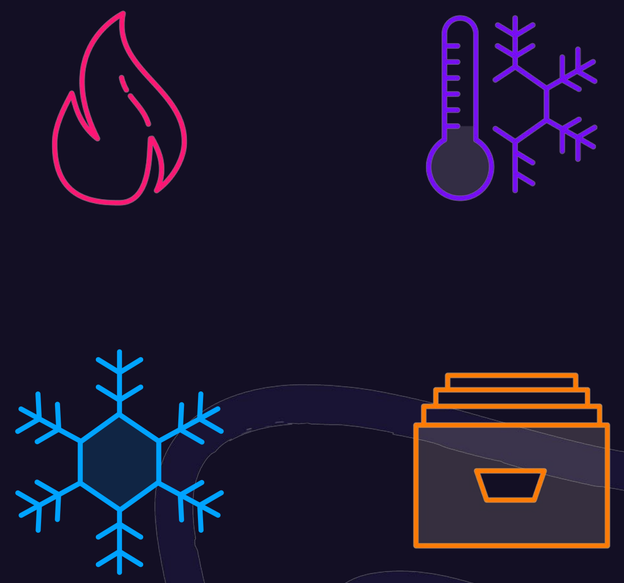
2. **Archive = offline data at huge discount**

   Requires several hours to get access

3. **Setting storage tiers**

   Account-level (default) = hot/cool/cold

   Blob-level = all types



Disks

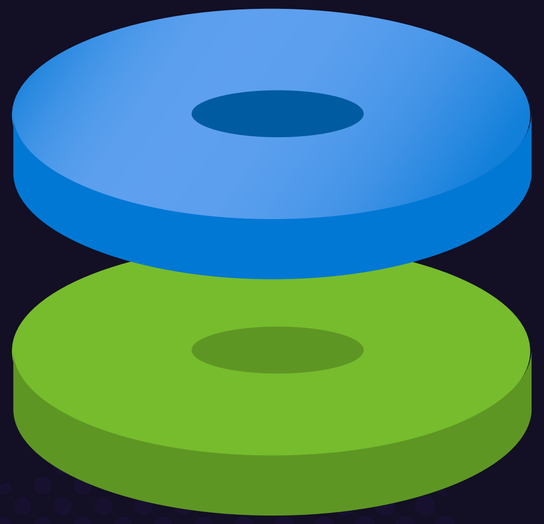
Managed Disks for Azure VMs

No Storage Account Information

Multiple performance options

HDD, Standard SSD, Premium SSD, Premium SSD v2, Ultra

VM must be in same region as disk



Azure Files

Fully Managed Cloud-based file share/server solution

1. **File server in the cloud**

2. **Synchronize or replace on-premises servers**

3. **Compatible with existing file server tools**

   PowerShell cmdlets, APIs

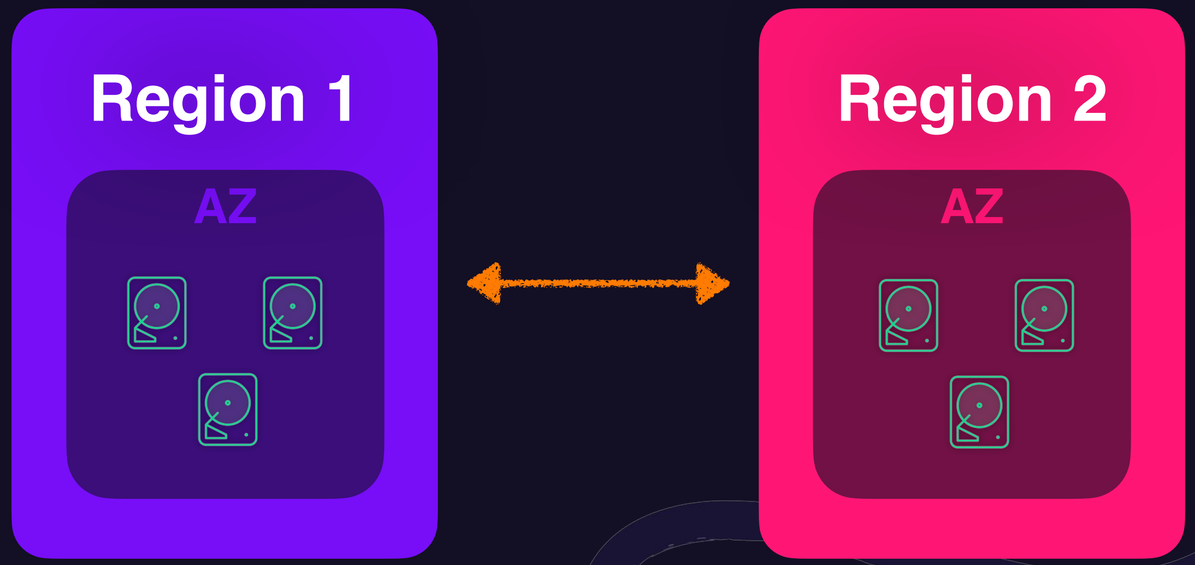
Storage Redundancy

Minimum three copies of data

Single/multiple zones/regions

Understand the acronyms

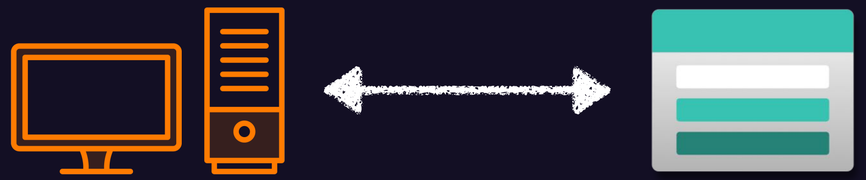
- LRS - Locally Redundant Storage
- ZRS - Zone-Redundant Storage
- GRS - Geo-Redundant Storage
- GZRS - Geo-Zone-Redundant Storage



Moving Data in Azure Storage

Know which tool works with which storage service

- AzCopy: Blobs and Azure Files
- Storage Explorer: All types
- Azure File Sync: Sync Azure Files



Know interface of tools

- AzCopy: Command-line
- Storage Explorer GUI interface

Additional Migration Options

Purpose of Data Box

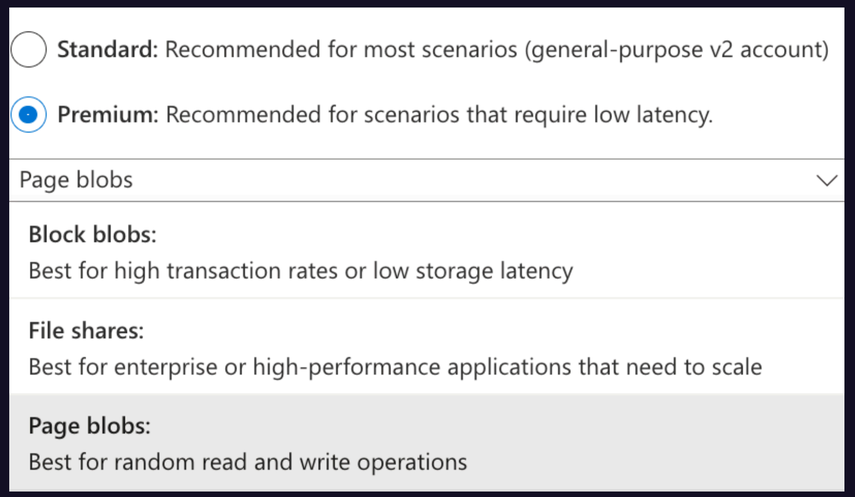
- Offline encrypted hard drive container
- Ship large amounts of data to be placed in storage account

Azure Migrate

- Migrate on-prem resources into Azure
  - Not just for storage accounts
- Migrate Servers, Databases, Applications

Exam Tips: Azure Storage

Premium Performance Options



General-purpose v2= standard performance, all service types

Know uses/restrictions of each premium option for <u>entire storage account</u>

- Premium block/page blobs: block/page blobs only
- Premium file shares: Azure Files only
- Redundancy Options: limited to single region for all
  - Page Blobs: LRS only

Course Summary

Matthew Ulasien
Azure Training Architect

What Did We Learn?

Architectural Components of Azure

Physical and Organization Management

Azure Compute

VMs and managed compute services

Azure Networking

VNets = central communication hub

Azure Storage

Multi-purpose data storage for many use cases

Next Steps

Continue your AZ-900 preparation!

AZ-900: Azure Security Management and Governance

Cost Management

Enforcing compliance standards

Managing and monitoring Azure resources

Get in Touch!

Submit feedback

Join the community!

Onwards!

See you in the next AZ-900 prep course!

Revisiting Defense in Depth

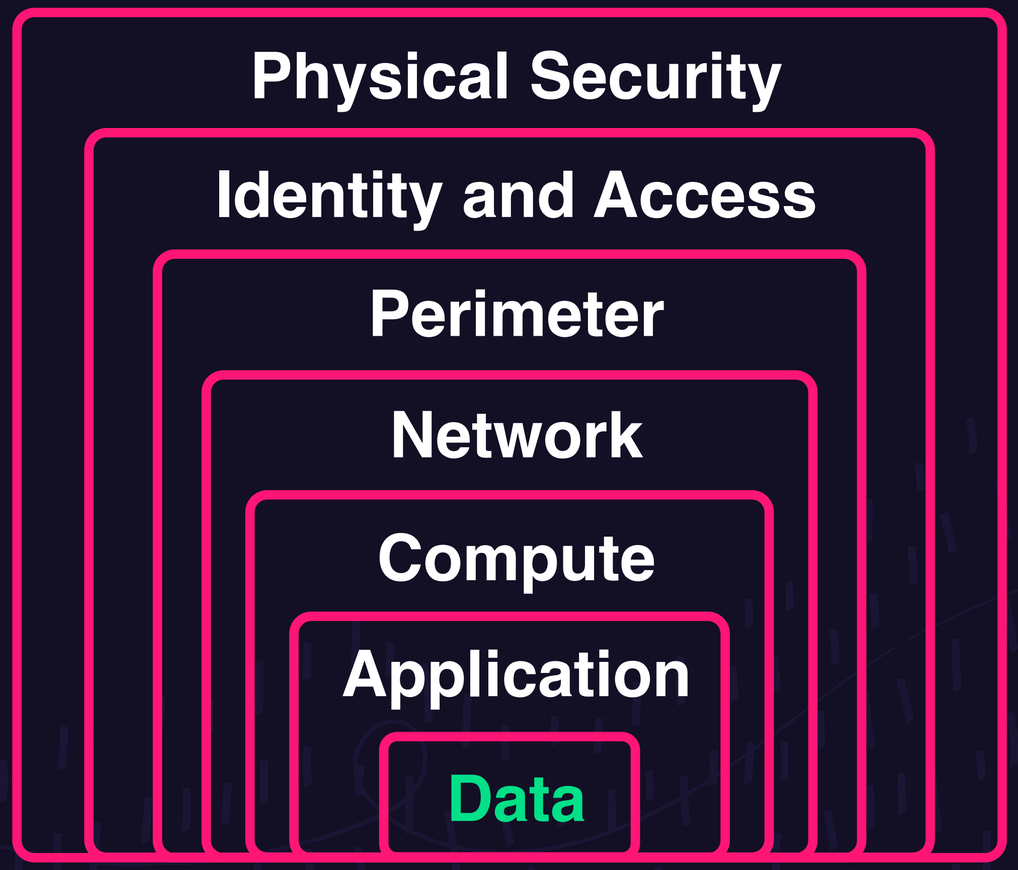
Matthew Ulasien
Azure Training Architect

Overview

OBJECTIVE: mitigate unauthorized data access

METHOD: layered defense

If one layer is breached, other layers can still stop attacks



Secure VMs and Managed Services

Compute

- Patch OSs
- Endpoint monitoring (anti-malware)

Identity and Access

- Secure logins/access keys
- Azure AD/Entra authentication
  - Fine-grained access with RBAC

Application

- Single Sign On (SSO)
- SSL encryption

Data

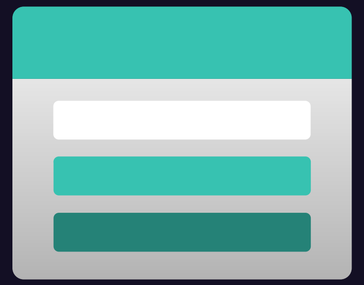
- Disk encryption
  - Default or custom

Secure Virtual Network Resources

Perimeter and Network

- Network Security Groups (NSGs)/Azure Firewall
- Private IP (no public exposure)
- Hybrid Networking
- DDoS Protection
- Subnets for isolation
- NSGs for traffic between subnets/ connected networks
- Network Peering
- Azure Bastion

Secure Storage Accounts



Identity and Access

- Manage public access to data
- RBAC for fine-grained access
- Access keys for other access methods

Perimeter and Network

- Private Endpoints - remove public exposure

Data

- Encryption
- Immutable Blob Storage - prevent changes