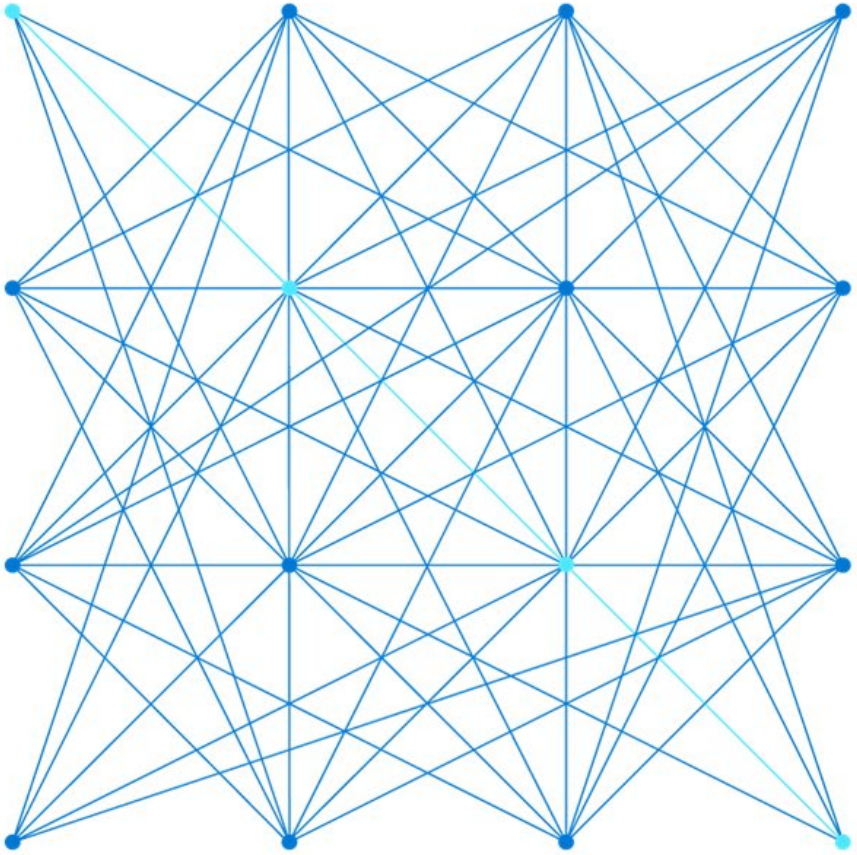
Microsoft Azure

Microsoft Azure Administrator

2 Days Webinar



Hello! Instructor Introduction

Instructor: Göran Eibel

Solution Architect

University Lecturer

Trainer

Author

goeran.eibel@gecon.at

About this course: Prerequisites

Successful Azure Administrators start this role with experience on operating systems, virtualization, cloud infrastructure, storage structures, and networking

Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks

Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies

Understanding of Active Directory concepts, such as users, groups, and role-based access control

Understanding of resilience and disaster recovery, including backup and restore operations

About this course: Course Outline

Module 01: Identity

Module 02: Governance and Compliance

Module 03: Azure Administration

Module 04: Virtual Networking

Module 05: Intersite Connectivity

Module 06: Network Traffic Management

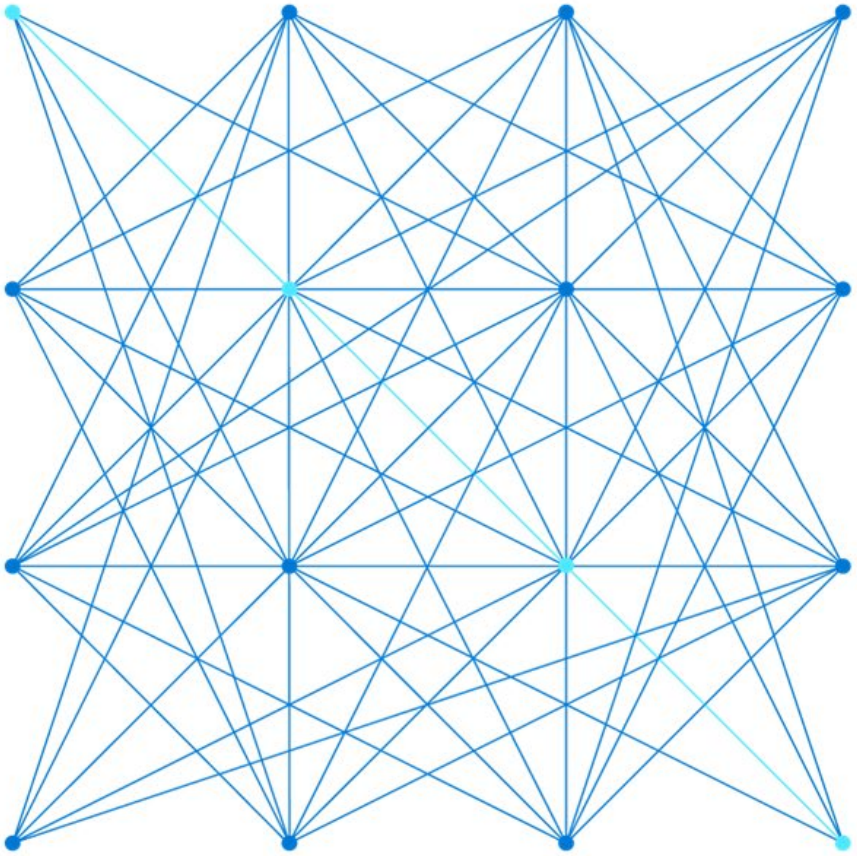
Module 07: Azure Storage

Module 08: Azure Virtual Machines

Module 09: Monitoring

Microsoft Azure

Module 01: Identity

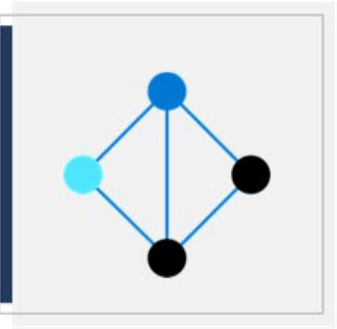


Module Overview

Lesson 01: Azure Active Directory

Lesson 02: Users and Groups

Lesson 01: Azure Active Directory



Azure Active Directory Overview

Azure Active Directory

Azure AD Concepts

AD DS vs. Azure Active Directory

Azure Active Directory Editions

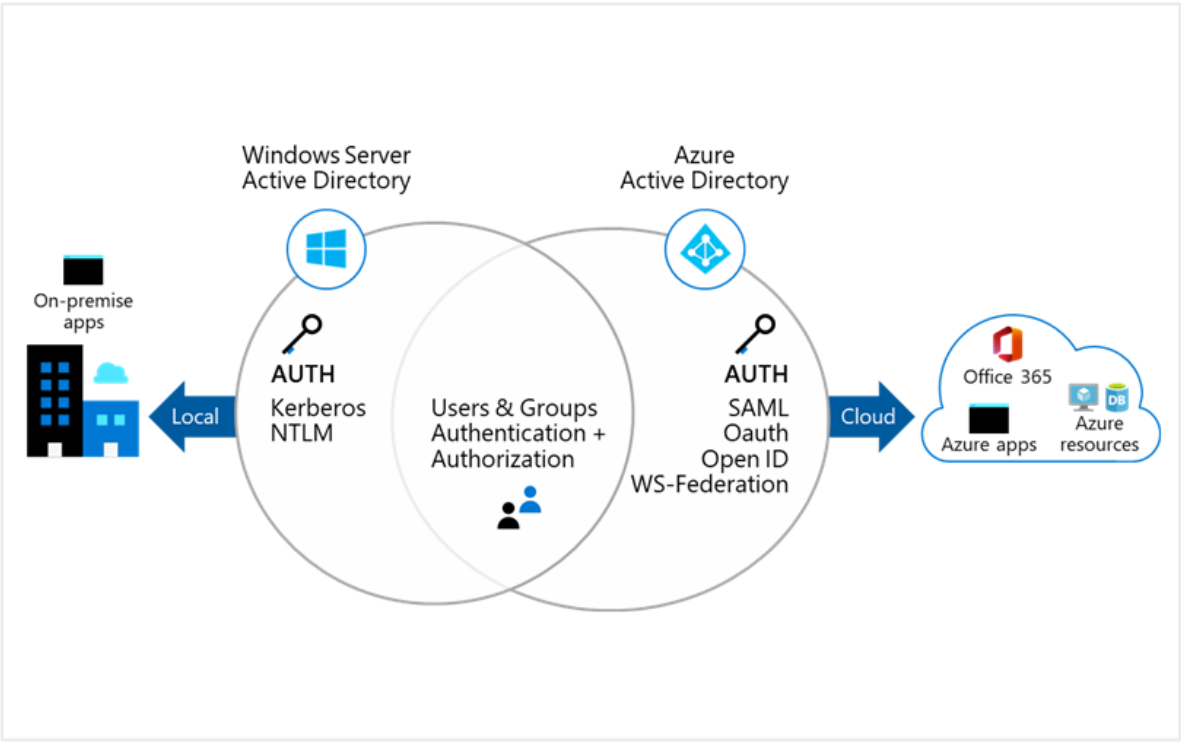
Azure AD Join

Self-Service Password Reset

Azure Active Directory

A cloud-based suite of identity management capabilities that enables you to securely manage access to Azure services and resources for your users

Provides application management, authentication, device management, and hybrid identity



Azure AD Concepts

Concept	Description
Identity	An object that can be authenticated
Account	An identity that has data associated with it
Azure AD account	An identity created through Azure AD or another Microsoft cloud service
Azure AD tenant	A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription
Azure AD directory	Each Azure tenant has a dedicated and trusted Azure AD directory
Azure subscription	Used to pay for Azure cloud services

AD DS vs Azure Active Directory

Azure AD is primarily an identity solution, and designed for HTTP and HTTPS communications

Queried using the REST API over HTTP and HTTPS. Instead of LDAP

Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization). Instead of Kerberos

Includes federation services, and many third-party services (such as Facebook)

Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)

Azure Active Directory Editions

Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

Azure AD Join

Single-Sign-On to your Azure managed SaaS apps and services

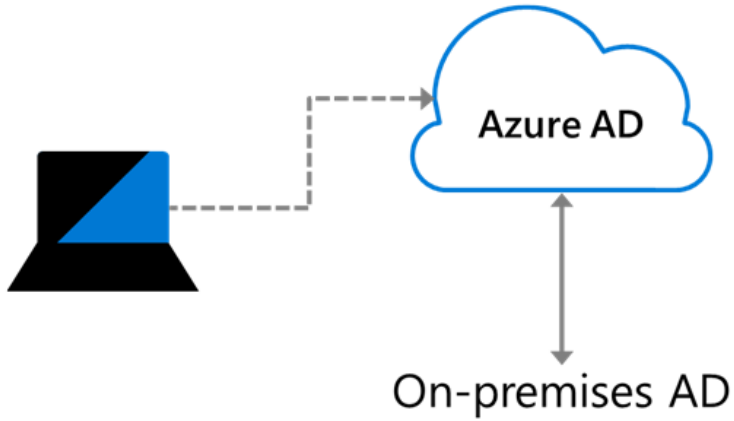
Enterprise compliant roaming of user settings across joined devices

Access to Microsoft Store for Business

Windows Hello support

Restriction of access to apps from only compliant devices

Seamless access to on-premises resources

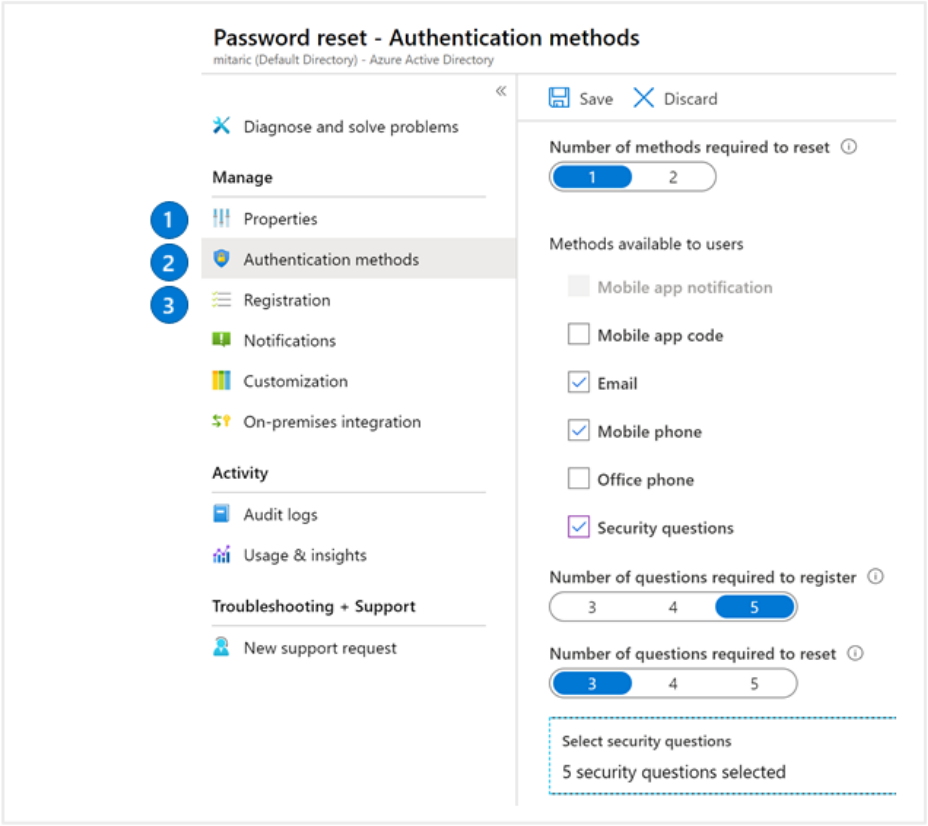


Self-Service Password Reset

1. Determine who can use self-service password reset

2. Choose the number of authentication methods required and the methods available (email, phone, questions)

3. You can require users to register for SSPR (same process as MFA)



Lesson 02: Users and groups

Users and Groups Overview

User Accounts

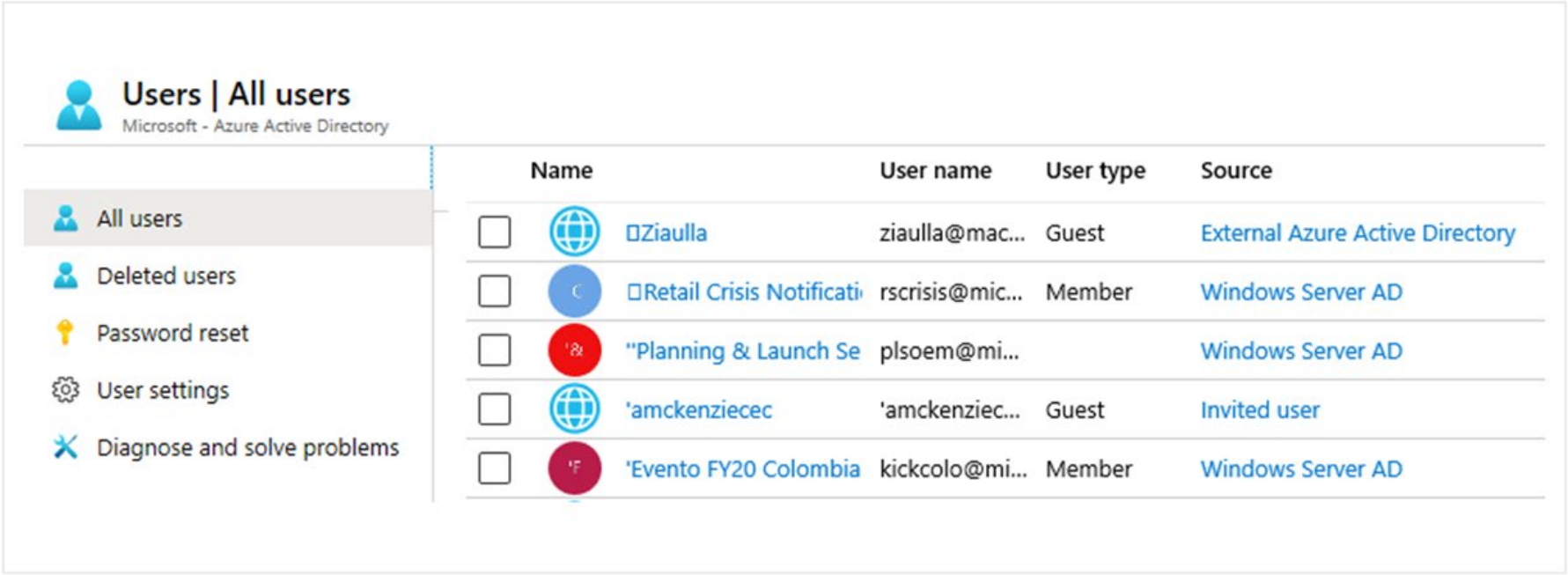
Managing User Accounts

Bulk User Accounts

Group Accounts

Managing Multiple Directories

User Accounts

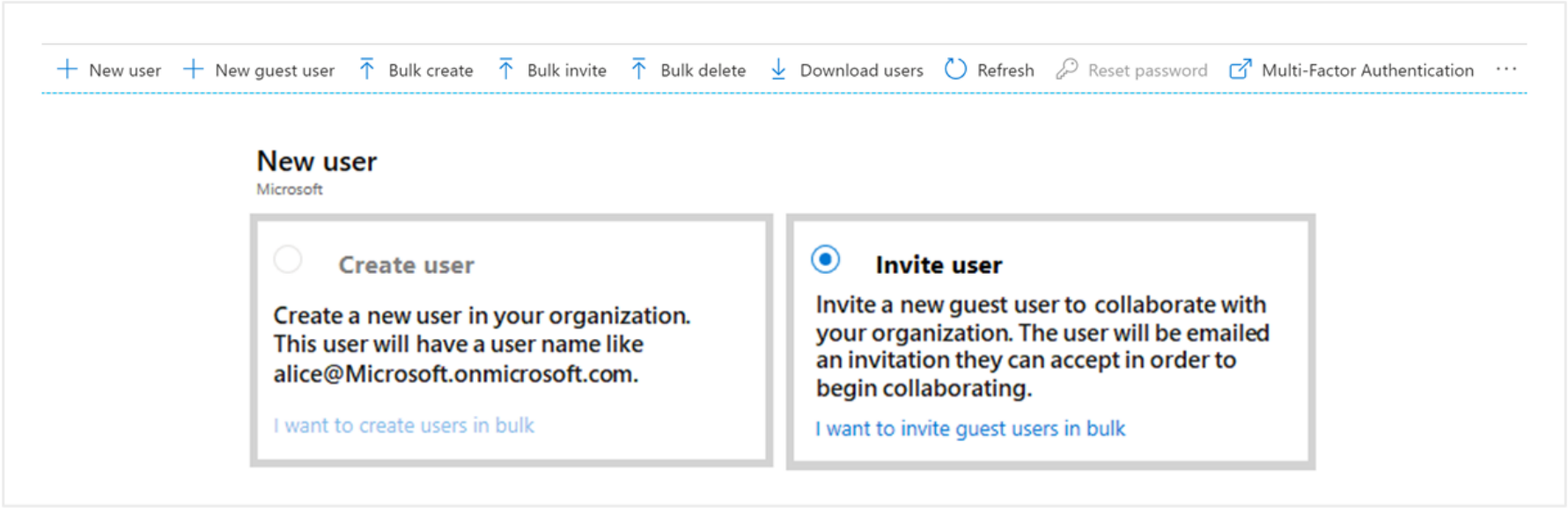


All users must have an account

The account is used for authentication and authorization

Identity Sources: Cloud, Directory-synchronized, and Guest

Managing User Accounts



Must be Global Administrator or User Administrator to manage users

User profile (picture, job, contact info) is optional

Deleted users can be restored for 30 days

Sign in and audit log information is available

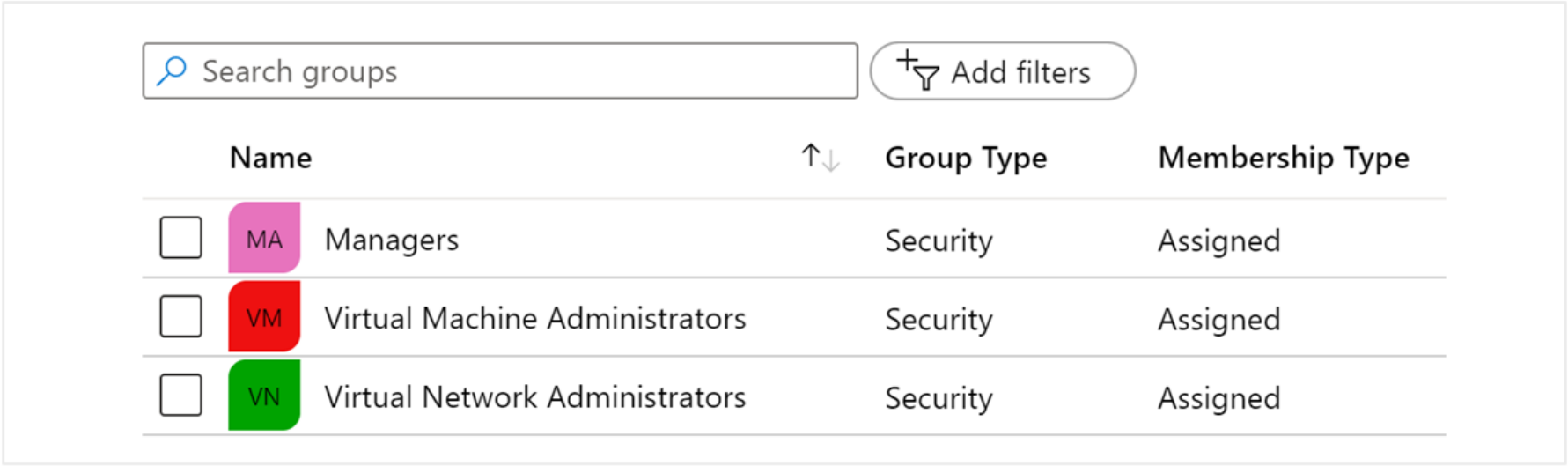
Bulk User Accounts

Create the comma-separated values (CSV) file with the list of all the users and their properties

Loop through the file processing each user

Consider error handling, duplicate users, initial password settings, empty properties, and when the account is enabled

Group Accounts



Group Types

- Security groups
- Office 365 groups

Assignment Types

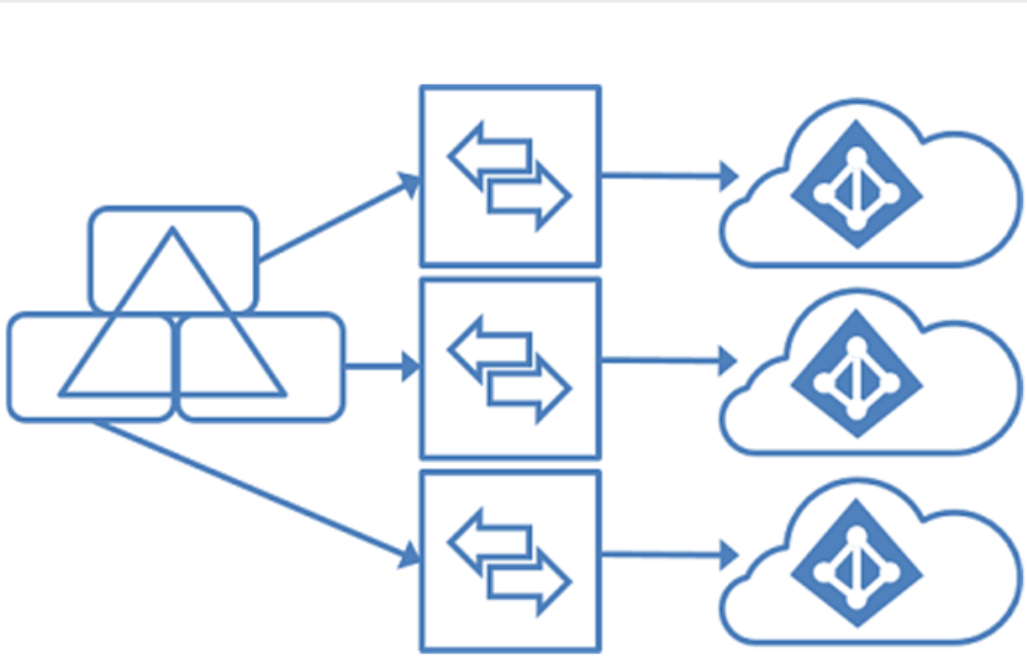
- Assigned
- Dynamic User
- Dynamic Device (Security groups only)

Managing Multiple Directories

In Azure Active Directory (Azure AD), each tenant is a fully independent resource

There is no parent-child relationship between tenants

This independence between tenants includes resource, administrative, and synchronization



✓ **It is recommended to use a supported synchronization configuration**

Microsoft Azure

Module 02: Governance and Compliance

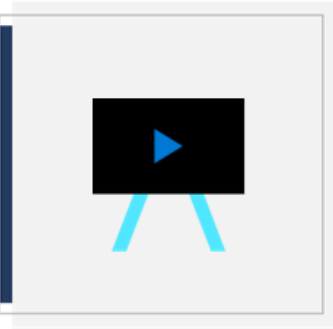
Module Overview

Lesson 01: Subscriptions and Accounts

Lesson 02: Azure Policy

Lesson 03: Role-Based Access Control

Lesson 01: Subscriptions and Accounts



Subscriptions and Accounts Overview

Regions

Azure Subscriptions

Getting a Subscription

Subscription Usage

Cost Management

Resource Tags

Cost Savings

Regions

- A region represents a collection of datacenters
- Provides flexibility and scale
- Preserves data residency
- Select regions close to your users
- Be aware of region deployment availability
- There are global services that are region independent
- Regions are paired for high availability

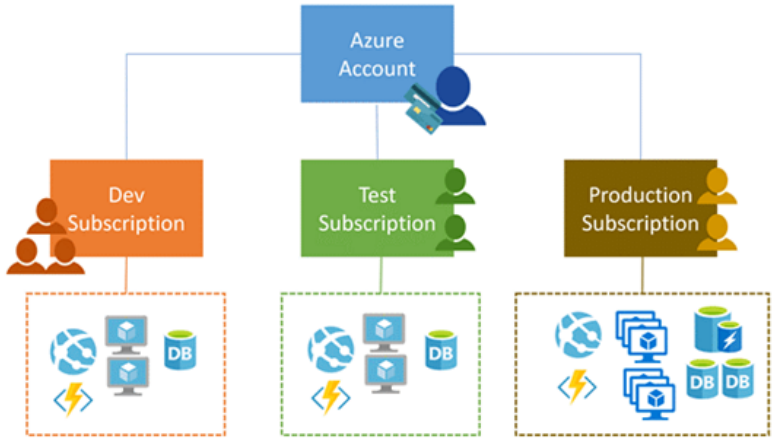
Worldwide there are 60+ regions representing 140 countries

Azure Subscriptions

Logical unit of Azure services that is linked to an Azure account

Security and billing boundary

Includes accounts – Identities in Azure Active Directory (Azure AD) or in a directory that is trusted by Azure AD, such as a work or school organization



Getting a Subscription

Enterprise Agreement customers make an upfront monetary commitment and consume services throughout the year

Resellers provide a simple, flexible way to purchase cloud services

Partners can design and implement your Azure cloud solution

Personal free account – Start right away

Subscription Usage

Subscription	Usage
Free	Includes a $200 credit for the first 30 days, free limited access for 12 months
Pay-As-You-Go	Charges you monthly
Enterprise	One agreement, with discounts for new licenses and Software Assurance – targeted at enterprise-scale organizations
Student	Includes $100 for 12 months – must verify student access

Cost Management

- Conduct cost analysis
- Create a budget
- Review recommendations
- Export the data

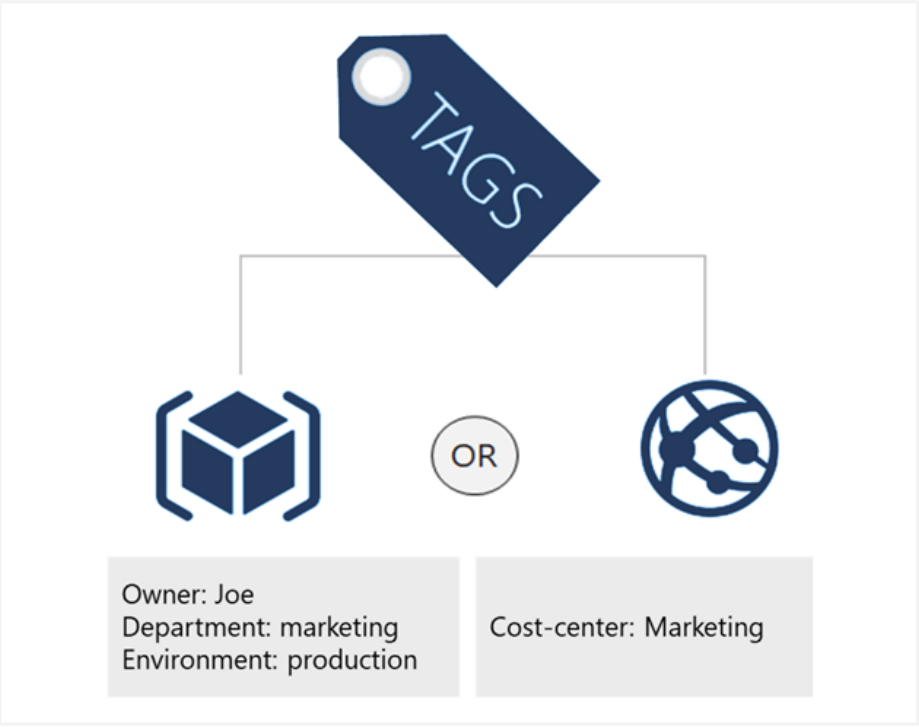
Resource Tags

Provides metadata for your Azure resources

Logically organizes resources into a taxonomy

Consists of a name-value pair

Very useful for rolling up billing information



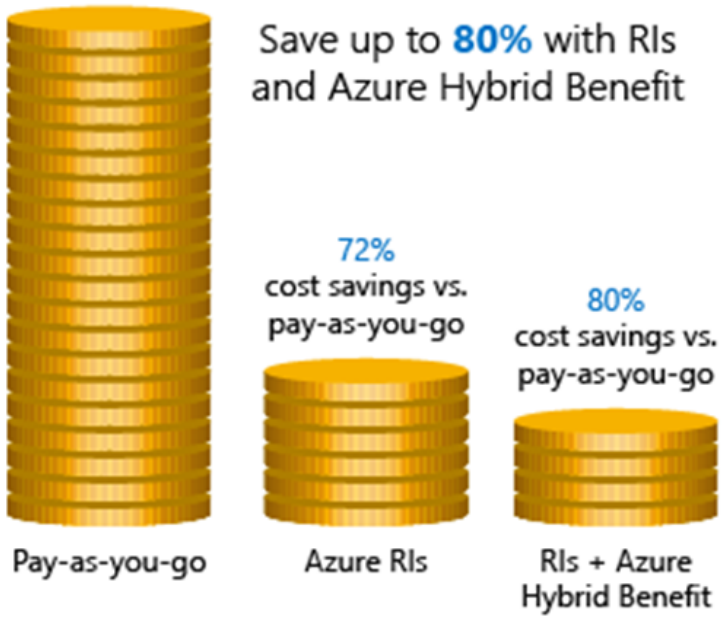
Cost Savings

Azure Reservations – Helps you save money by pre-paying for services

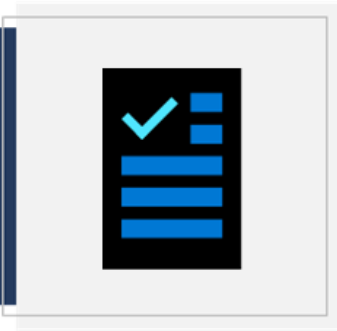
Azure Hybrid Benefits – Use Windows Server and SQL Server on-premises licenses with Software Assurance

Azure Credits – Monthly credit benefit that allows you to experiment with, develop, and test new solutions on Azure

Regions – Choose low-cost locations and regions



Lesson 02: Azure Policy



Azure Policy Overview

Management Groups

Azure Policy

Implementing Azure Policy

Policy Definitions

Create Initiative Definitions

Scope the Initiative Definition

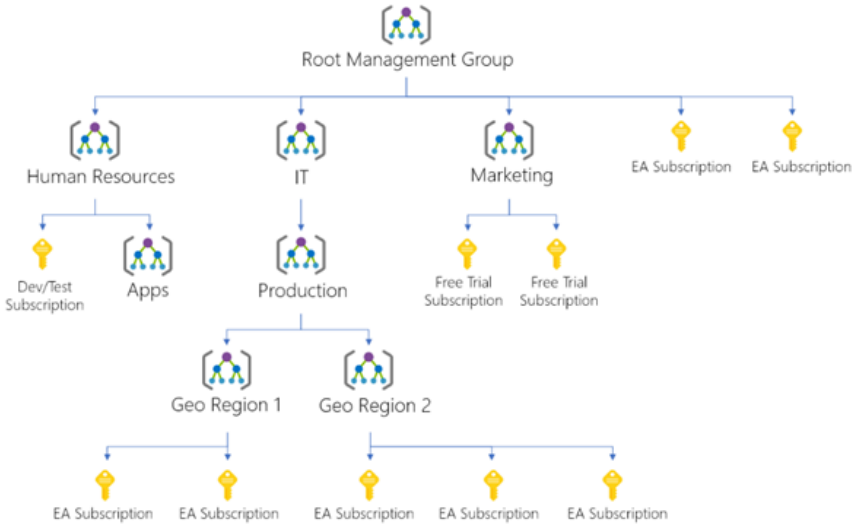
Determine Compliance

Management Groups

Provides a level of scope above subscriptions

Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies

Compliance and cost reporting by organization (business/teams)



Azure Policy

Azure Policy is a service in Azure that you use to create, assign and, manage policies

Azure Policy runs evaluations and scans for non-compliant resources

Advantages:

Enforcement and compliance

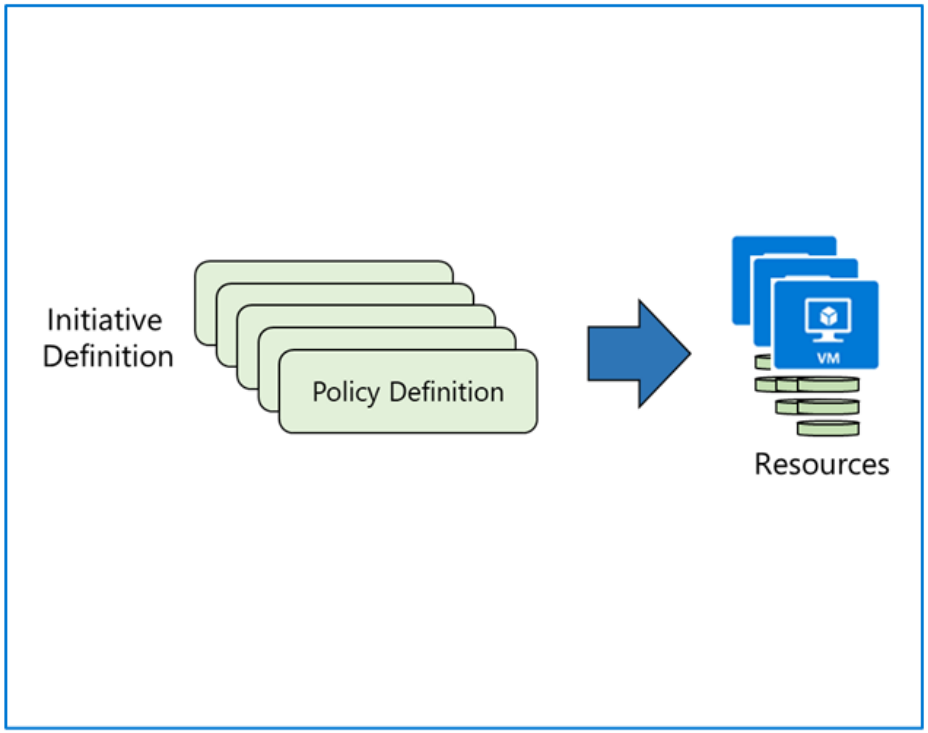
Apply policies at scale

Remediation

Usage Cases
Allowed resource types – Specify the resource types that your organization can deploy
Allowed virtual machine SKUs – Specify a set of virtual machine SKUs that your organization can deploy
Allowed locations – Restrict the locations your organization can specify when deploying resources
Require tag and its value – Enforces a required tag and its value
Azure Backup should be enabled for Virtual Machines – Audit if Azure Backup service is enabled for all Virtual machines

Implementing Azure Policy

1. Browse Policy Definitions
2. Create Initiative Definitions
3. Scope the Initiative Definition
4. View Policy evaluation results



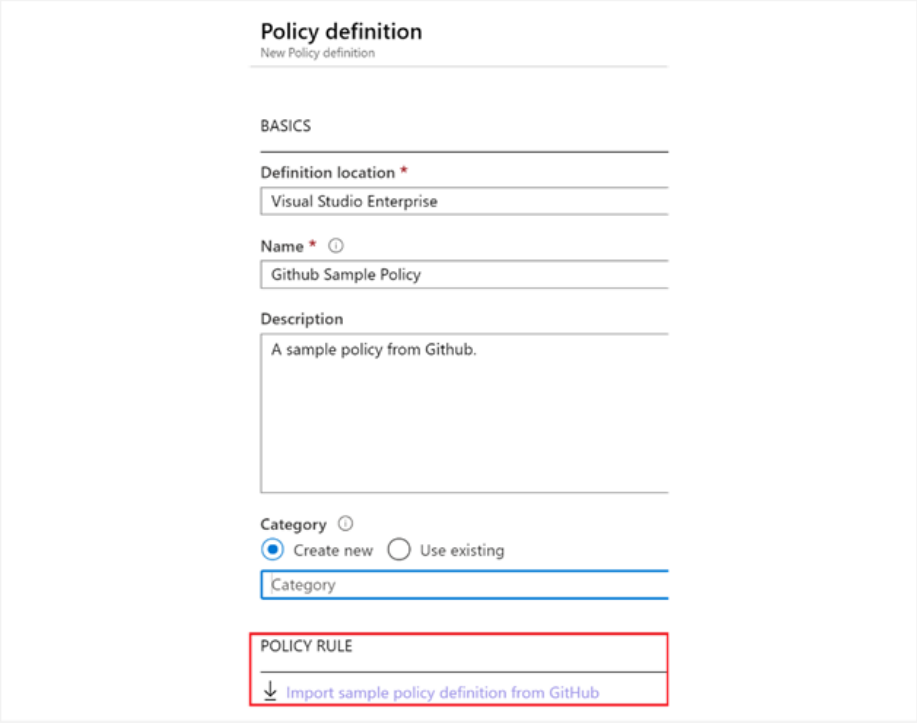
Policy Definitions

Many policy definitions are available

You can import policies from GitHub

Policy Definitions have a specific JSON format

You can create custom policy definitions

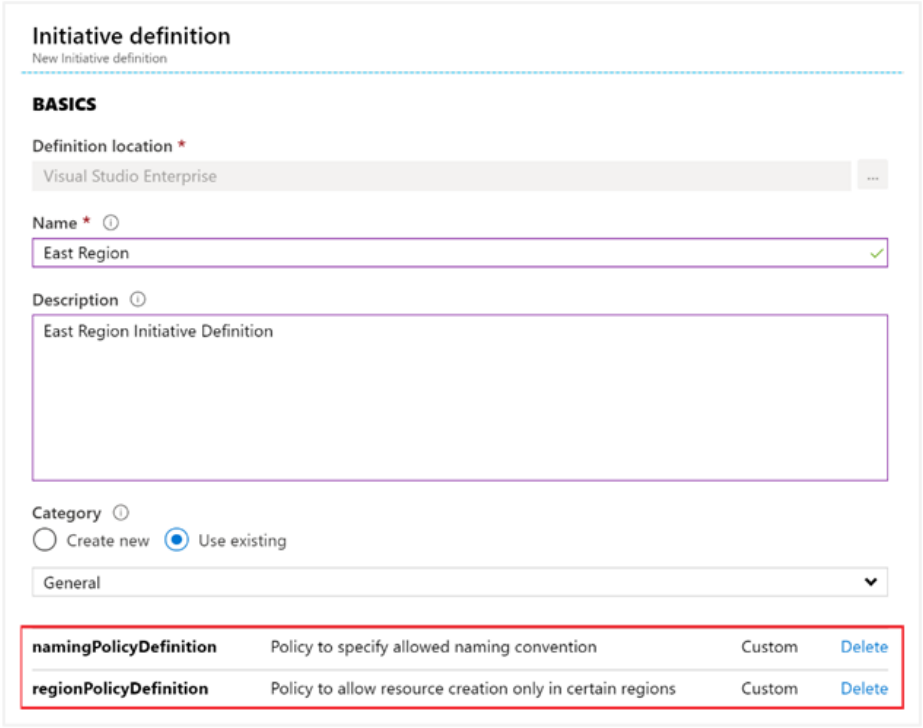


Create Initiative Definitions

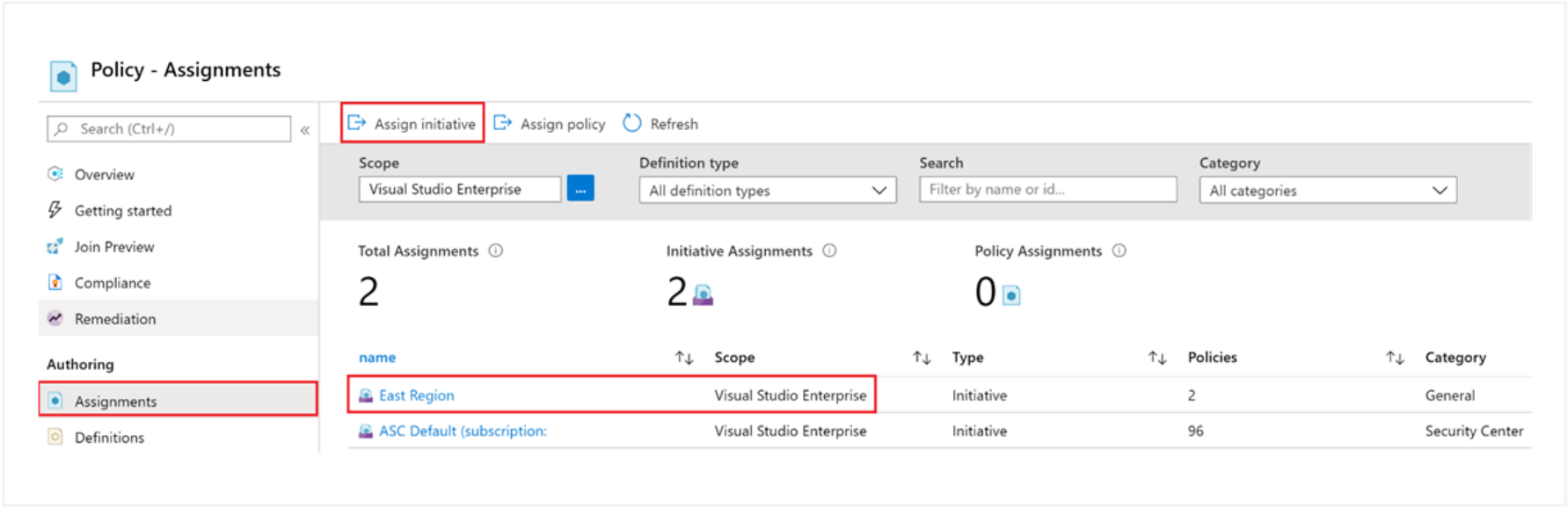
Group policy definitions

Include one or more policies

Requires planning



Scope the Initiative Definition

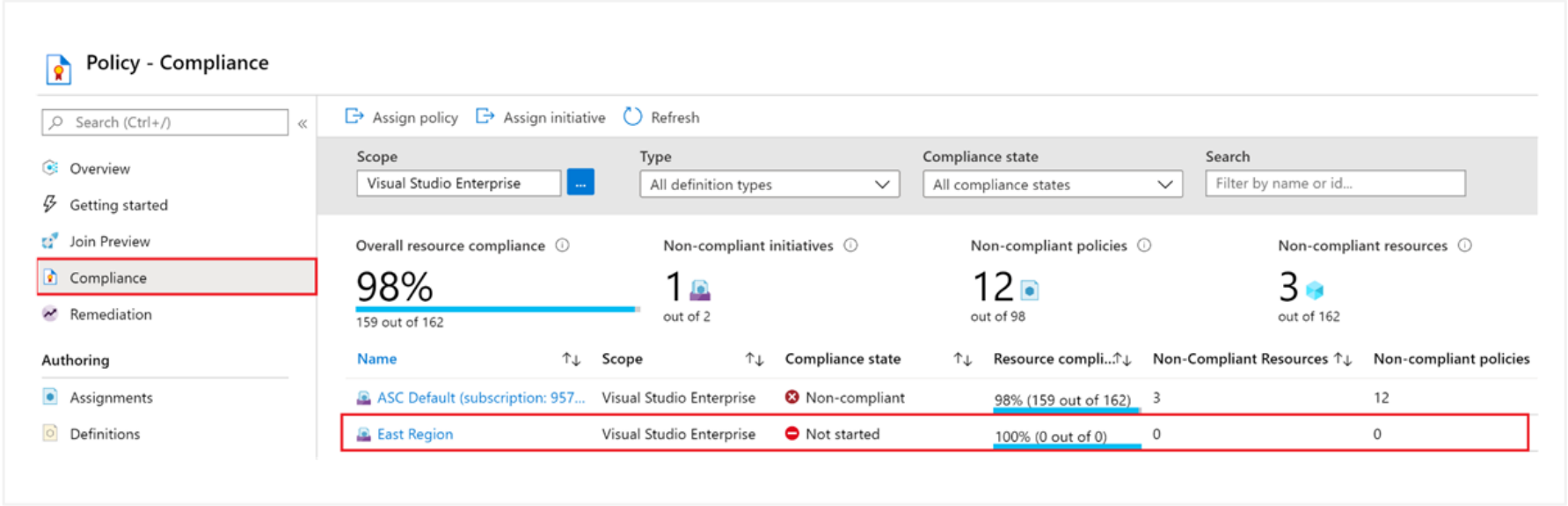


Assign the definition to a scope

The scope enforces the policy

Select the subscription, and optionally the resource group

Determine Compliance



Non-compliant initiatives

Non-compliant policies

Non-compliant resources

Lesson 03: Role-Based Access Control

Role-Based Access Control Overview

Role-Based Access Control

Role Definition

Role Assignment

Azure RBAC Roles vs Azure AD Administrator Roles

RBAC Authentication

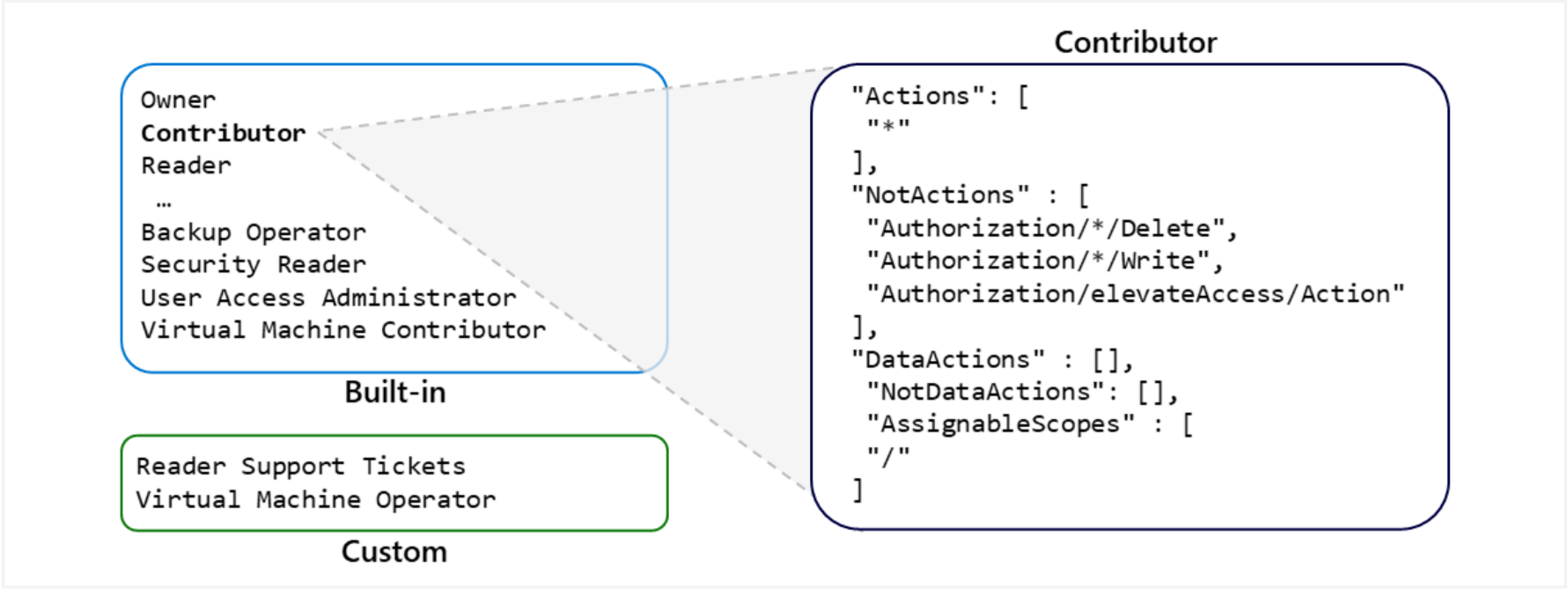
Azure RBAC Roles

Role-Based Access Control

Provides fine-grained access management of resources in Azure	Concepts
Built on Azure Resource Manager Segregate duties within your team Grant only the amount of access to users that they need to perform their jobs	**Security principal**. Object that represents something that is requesting access to resources **Role definition.** Collection of permissions that lists the operations that can be performed **Scope.** Boundary for the level of access that is requested **Assignment.** Attaching a role definition to a security principal at a particular scope: • Users can grant access described in a role definition by creating an assignment • Deny assignments are currently read-only and are set by Azure Blueprints and Azure Managed Apps

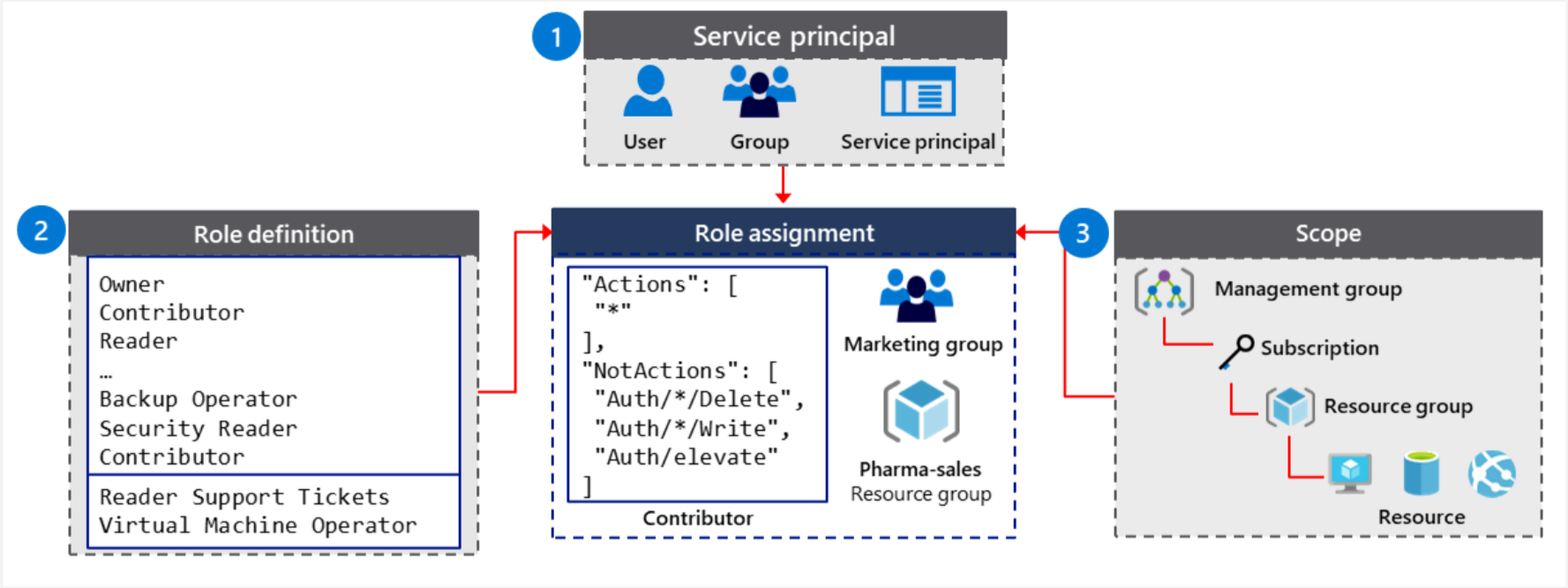
Role Definition

Collection of permissions that lists the operations that can be performed



Role Assignment

Process of binding a role definition to a user, group, or service principal at a scope for the purpose of granting access



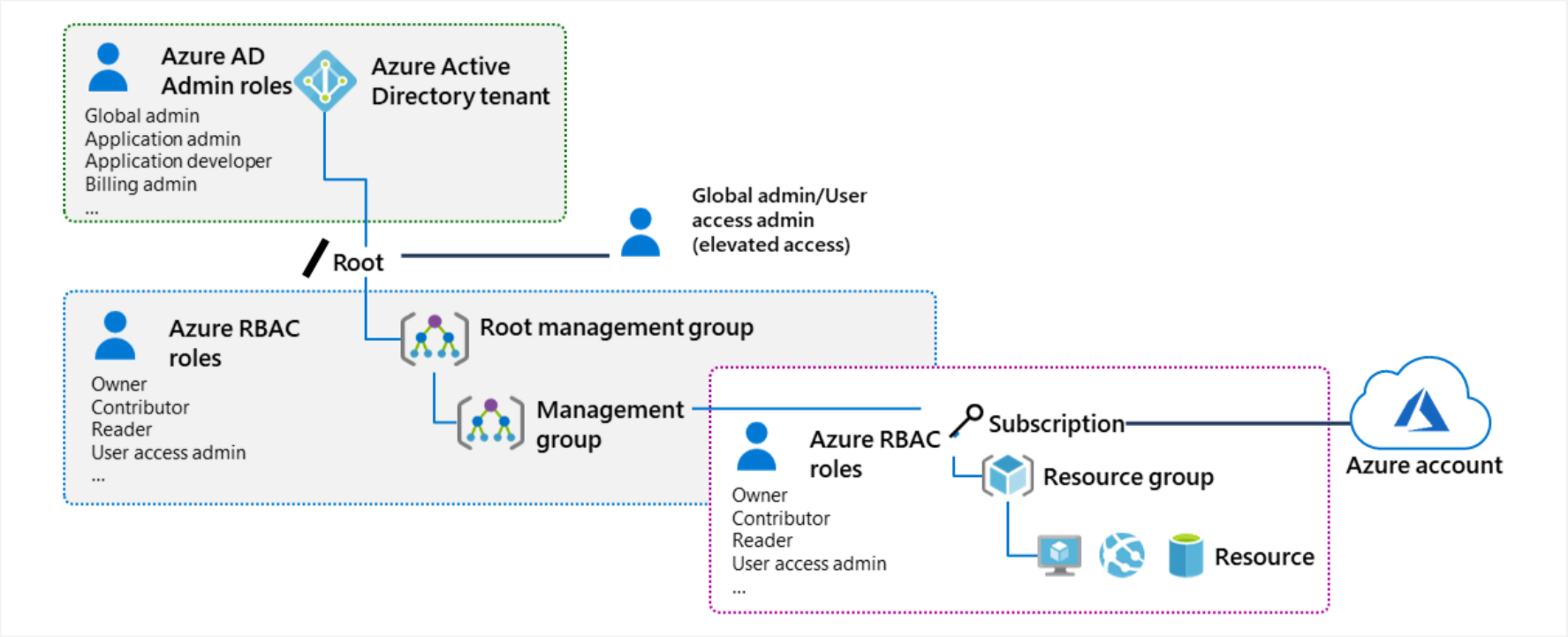
Azure RBAC Roles vs. Azure AD Roles

Azure and Azure AD offer two types of roles

Azure RBAC roles	Azure AD roles
Manage access to Azure resources	Manage access to Azure AD objects
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure portal, Office 365 admin portal, Microsoft Graph, Azure Active Directory PowerShell for Graph

Classic administrator roles should be avoided if using Azure Resource Manager

RBAC Authentication

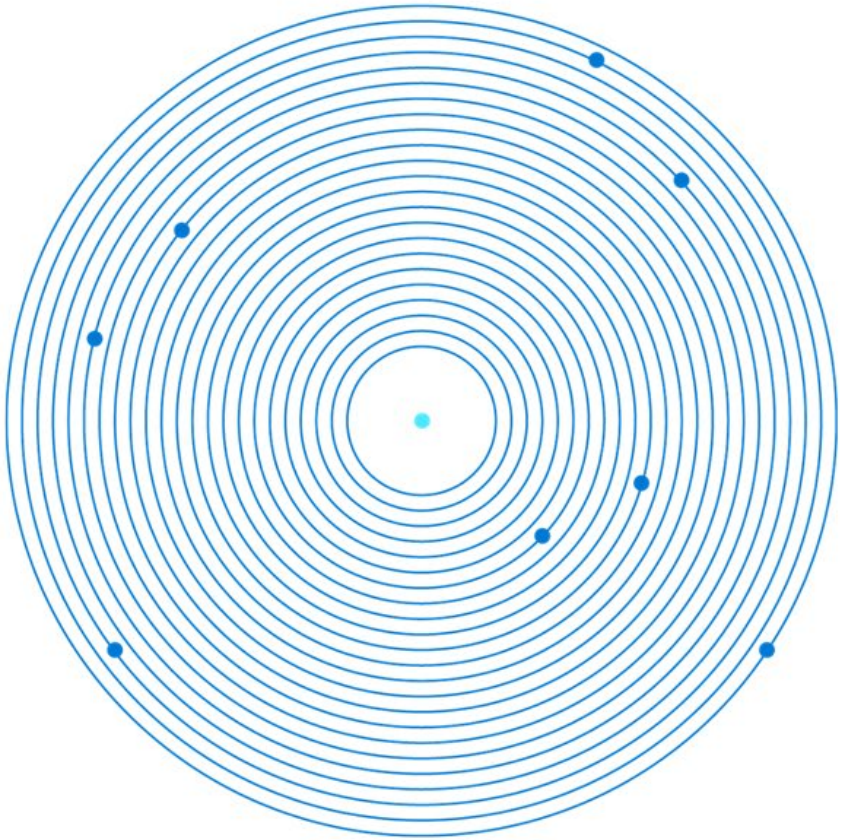


Azure RBAC Roles

RBAC role in Azure	Permissions	Notes
Owner	Has full access to all resources and can delegate access to others	The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope. This applies to all resource types
Contributor	Creates and manages all types of Azure resources but cannot grant access to others	This applies to all resource types
Reader	Views Azure resources	This applies to all resource types
User Access Administrator	Manages user access to Azure resources	This applies to managing access, rather than to managing resources

Microsoft Azure

Module 03: Azure Administration



Module Overview

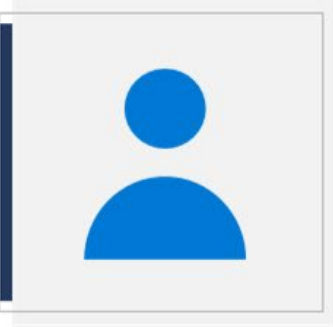
Lesson 01: Resource Manager

Lesson 02: Azure Portal and Cloud Shell

Lesson 03: Azure PowerShell and CLI

Lesson 04: ARM Templates

Lesson 01: Resource Manager



Resource Manager Overview

Resource Manager

Terminology

Resource Group Deployments

Resource Manager Locks

Moving Resources

Removing Resources and Resource Groups

Resource Limits

Resource Manager

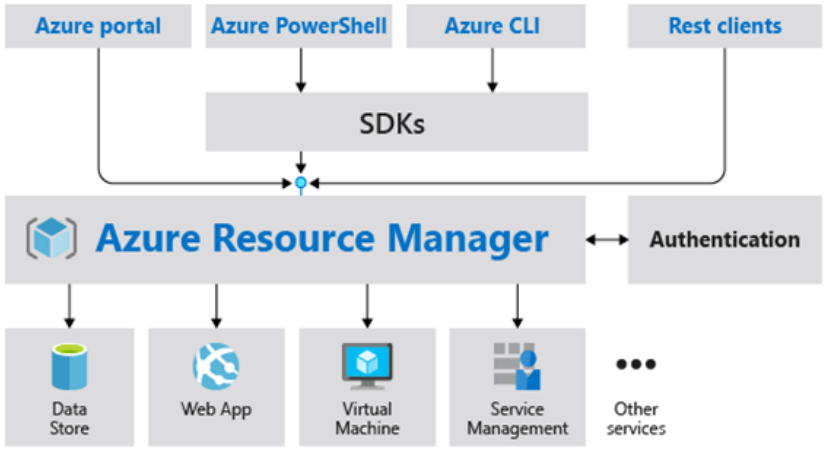
Provides a consistent management layer

Enables you to work with the resources in your solution as a group

Deploy, update, or delete in a single, coordinated operation

Provides security, auditing, and tagging features

Choose the tools and APIs that work best for you



Terminology

A **resource** is simply a single service instance in Azure

A **resource group** is a logical grouping of resources

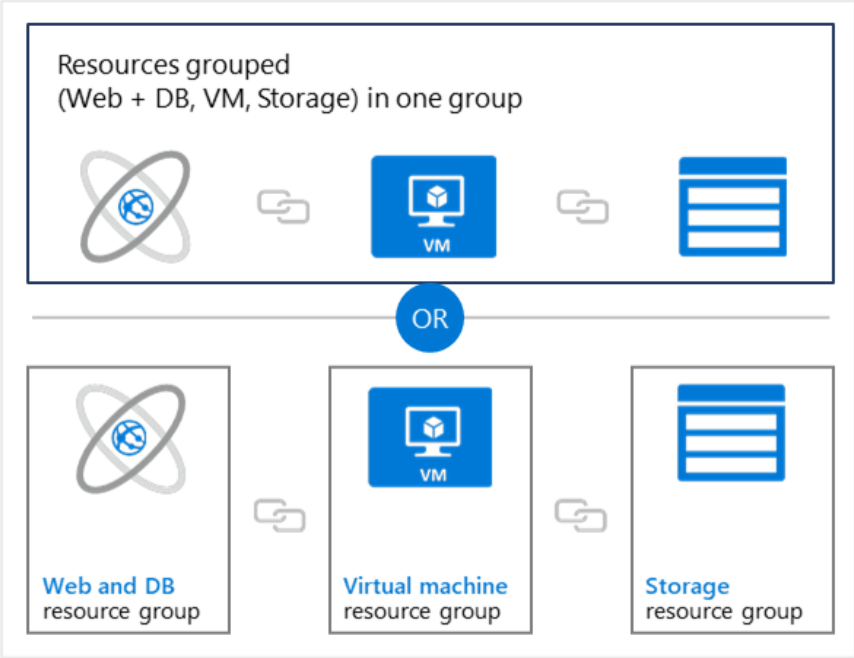
An **Azure Resource Manager template** is a JSON file that allows you to declaratively describe a set of resources

A **declarative syntax** is what a template uses to state what you intend to create

A **resource provider** is service that supplies the resources you can deploy and manage through Resource Manager

Resource Group Deployments

- Resources can only exist in one resource group
- Groups cannot be renamed
- Groups can have resources of many different types (services)
- Groups can have resources from many different regions
- Deployments are incremental



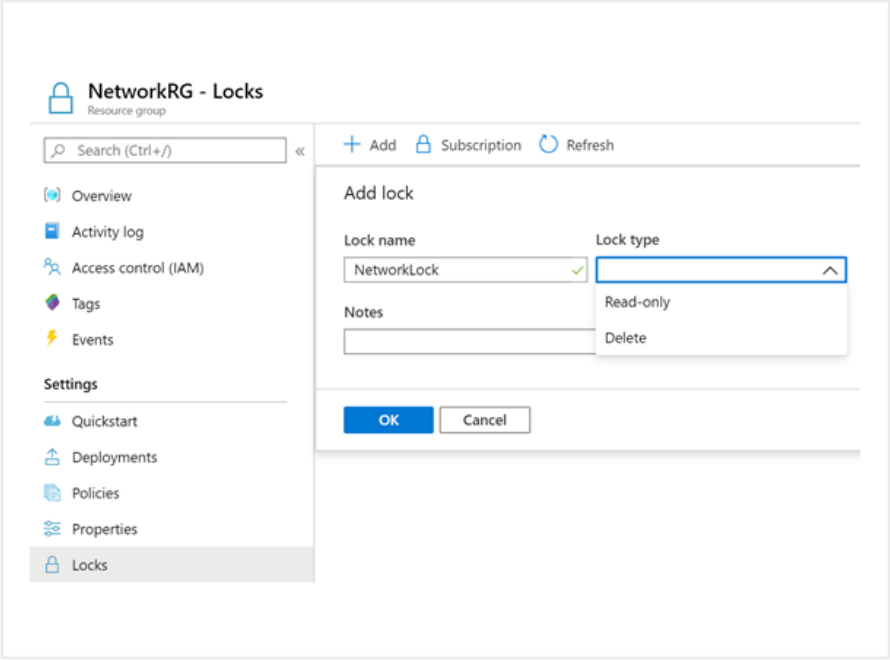
Resource Manager Locks

Associate the lock with a subscription, resource group, or resource

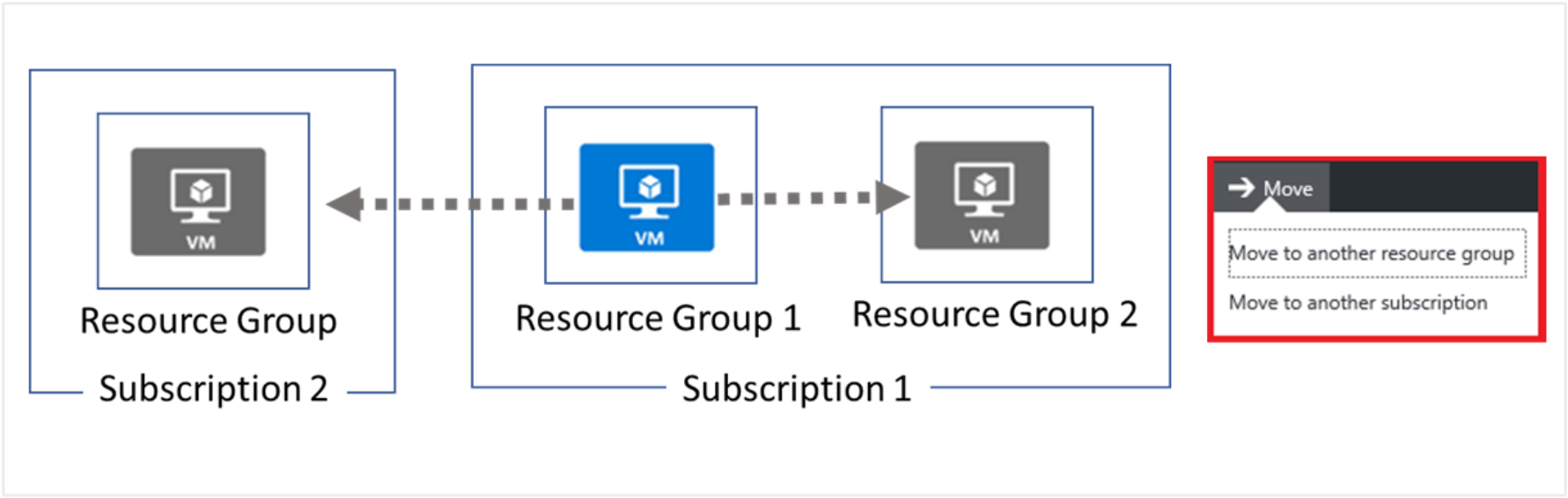
Locks are inherited by child resources

Read-Only locks prevent any changes to the resource

Delete locks prevent deletion



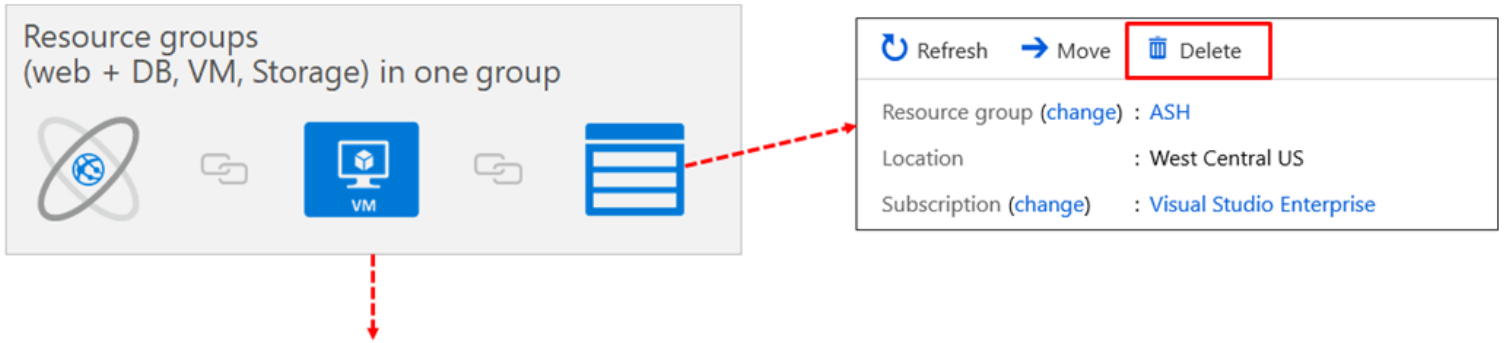
Moving Resources



When moving resources, both the source group and the target group are locked during the operation

Services that cannot be moved: Azure AD Domain Services, ExpressRoute, and Site Recovery. Other restrictions apply

Removing Resources and Resource Groups



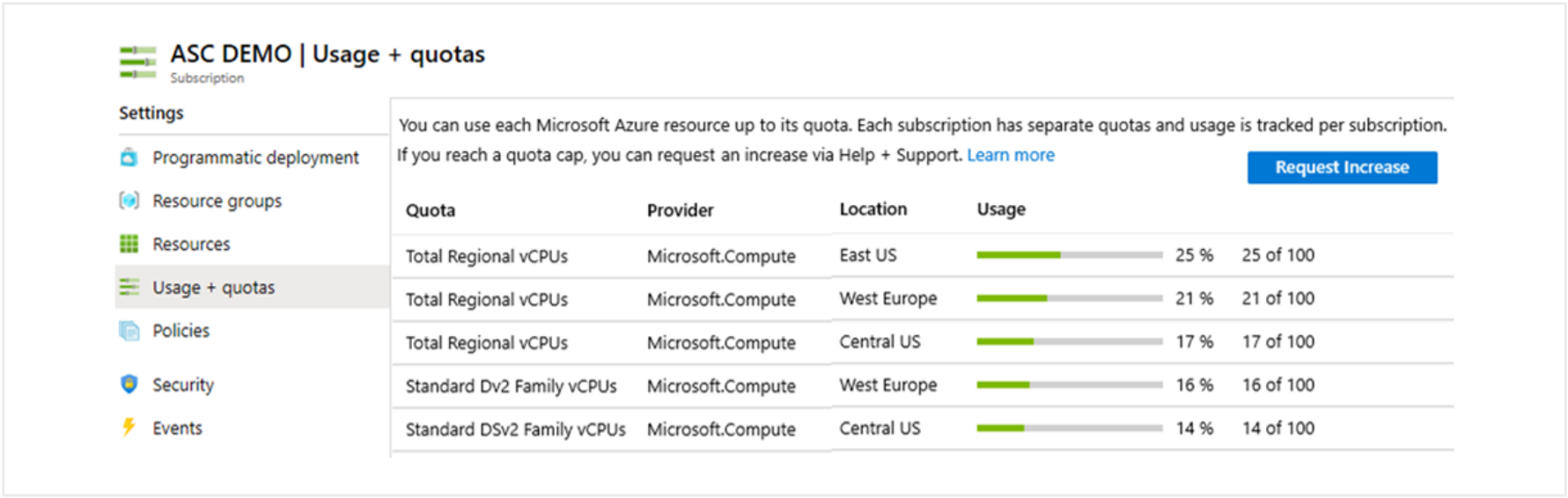

```
Get-AzResourceGroup -Name 'az104-03*' | Remove-AzResourceGroup -Force -AsJob
```

Remove Azure resources that you no longer use

Ensures you will not see unexpected charges

Remove individual resources or remove the resource group

Resource Limits



Resources have a default limit also known as quota

Helpful to track current usage, and plan for future use

You can open a free support case to increase limits to published maximums

Lesson 02: Azure Portal and Cloud Shell

Azure Portal and Cloud Shell overview

Azure Portal

Demonstration – Azure Portal

Azure Cloud Shell

Azure Portal

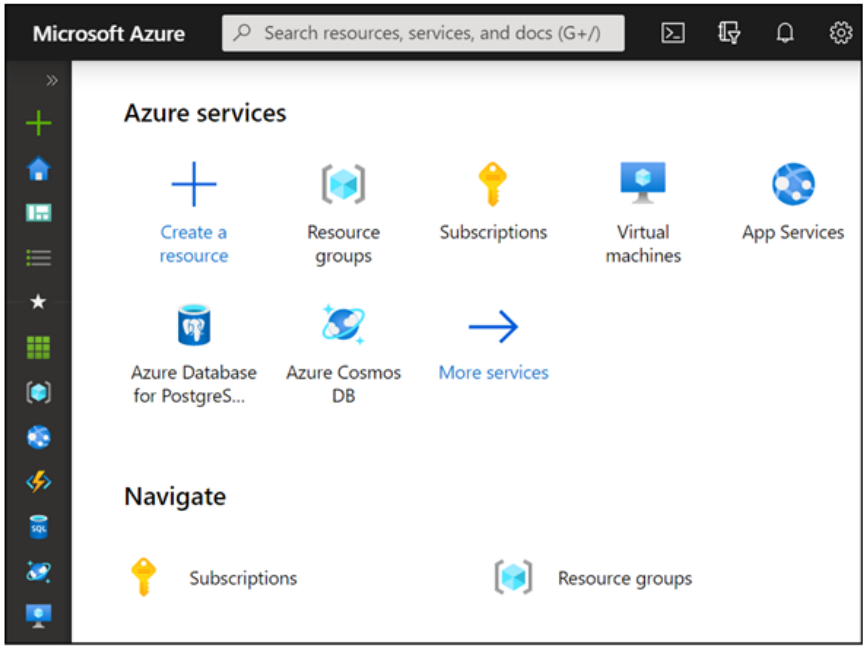
Search resources, services, and docs

Manage resources

Create customized dashboards and favorites

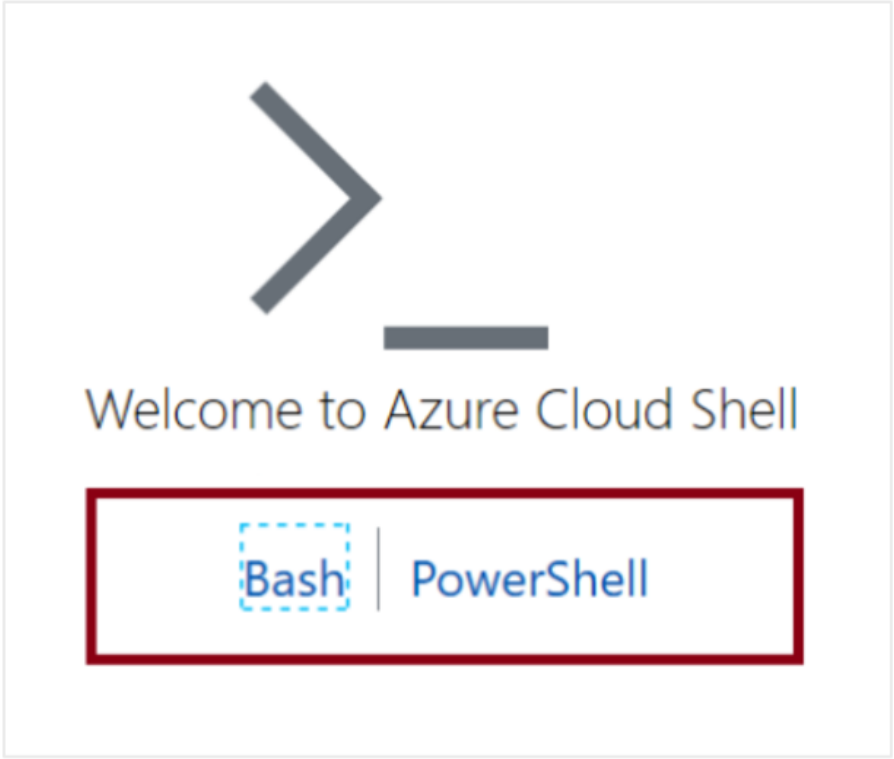
Access the Cloud Shell

Receive notifications

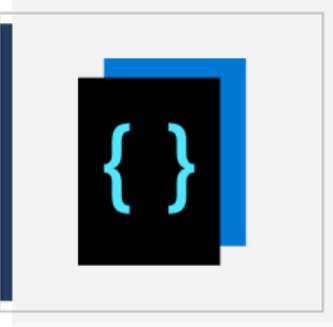


Azure Cloud Shell

- Interactive, browser-accessible shell
- Offers either Bash or PowerShell
- Is temporary and provided on a per-session, per-user basis
- Requires a resource group, storage account, and Azure File share
- Authenticates automatically
- Integrated graphical text editor
- Is assigned one machine per user account
- Times out after 20 minutes



Lesson 03: Azure PowerShell and CLI



Azure PowerShell and CLI Overview

Azure PowerShell

PowerShell Cmdlets and Modules

Demonstration – Working with PowerShell locally

Azure CLI

Azure PowerShell

```
New-AzVm `
  -ResourceGroupName "CrmTestingResourceGroup" `
  -Name "CrmUnitTests" `
  -Image "UbuntuLTS" `
...
```

Connect to your Azure subscription and manage resources

Adds the Azure-specific commands

Available inside a browser via the Azure Cloud Shell

Available as a local installation on Linux, macOS, or Windows

Has an interactive and a scripting mode

PowerShell Cmdlets and Modules

```
Get-Module
# Output
ModuleType Version    Name
---------- -------    ----
Manifest   3.1.0.0    Microsoft.PowerShell.Management
Manifest   3.1.0.0    Microsoft.PowerShell.Utility
Binary     1.0.0.1     PackageManagement
Script     1.0.0.1     PowerShellGet
Script     2.0.0      PSReadline
```

Cmdlets follow a verb-noun naming convention; shipped in modules

Modules are a DLL file with the code to process each cmdlet

Load cmdlets by loading the module containing them

Use **Get-Module** to see a list of loaded modules

Azure CLI

```
az vm restart -g MyResourceGroup -n MyVm
```

Cross-platform command-line program

Runs on Linux, macOS, and Windows

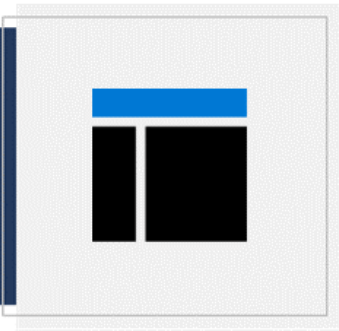
Can be used interactively or through scripts

Commands are structured in *groups* and *subgroups*

Use *find* to locate commands

Use *--help* for more detailed information

Lesson 04: ARM templates



ARM Templates Overview

Template Advantages

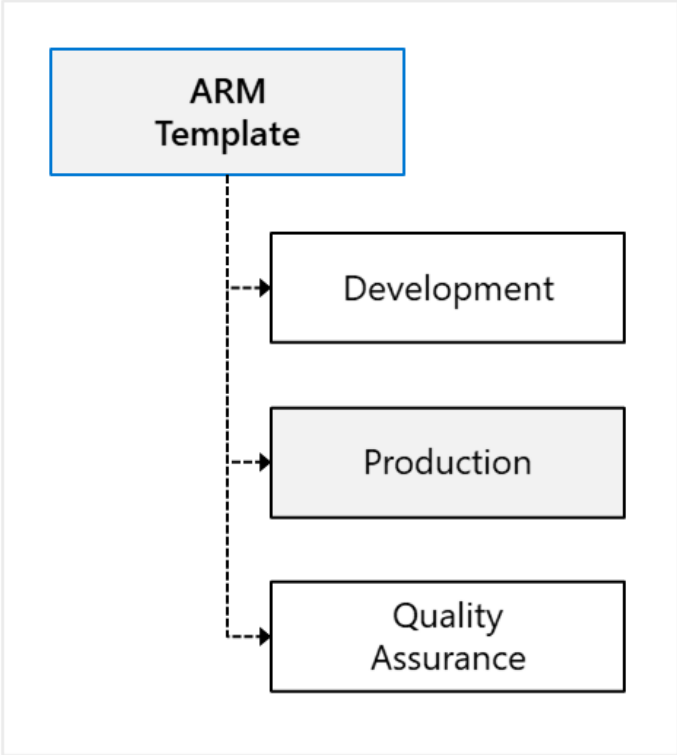
Template Schema

Template Parameters

QuickStart Templates

Template Advantages

- Improves consistency
- Express complex deployments
- Reduce manual, error prone tasks
- Express requirements through code
- Promotes reuse
- Modular and can be linked
- Simplifies orchestration



Template Schema

Defines all the Resource manager resources in a deployment

Written in JSON

A collection of key-value pairs

Each key is a string

Each values can be a string, number, Boolean expression, list of values, object

```
{
    "$schema":
      "http://schema.management.
      azure.com/schemas/2019-04-
      01/deploymentTemplate.json#",
    "contentVersion": "",
    "parameters": {},
    "variables": {},
    "functions": [],
    "resources": [],
    "outputs": {}
}
```

Template Parameters

Specify which values are configurable when the template runs

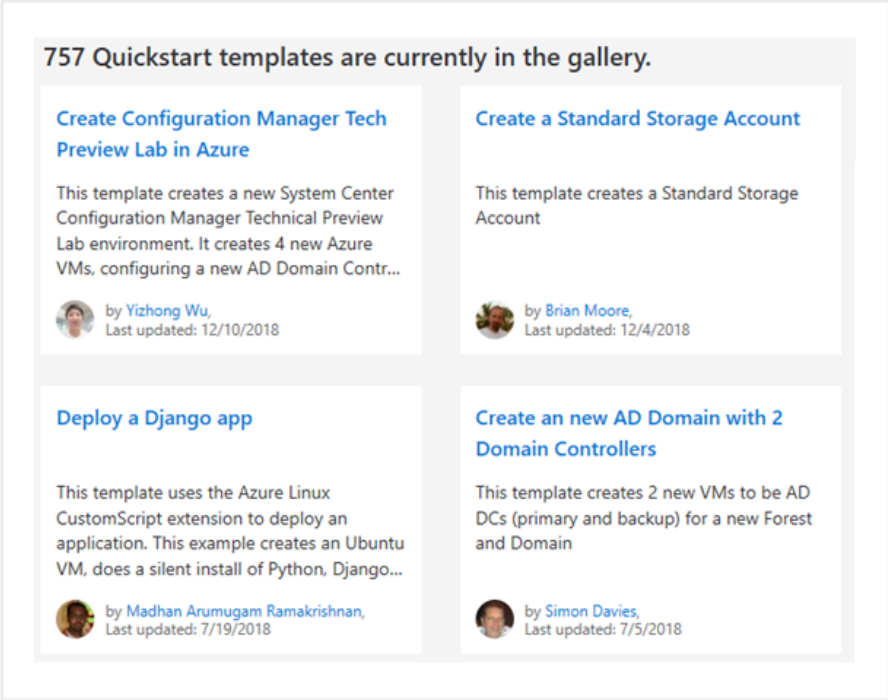
This example has two parameters: one for a VM's username (adminUsername), and one for its password (adminPassword)

```
"parameters": {
  "adminUsername": {
    "type": "string",
    "metadata": {
      "description": "Username for the VM."
    }
  },
  "adminPassword": {
    "type": "securestring",
    "metadata": {
      "description": "Password for the VM."
    }
  }
}
```

QuickStart Templates

Resource Manager templates provided by the Azure community

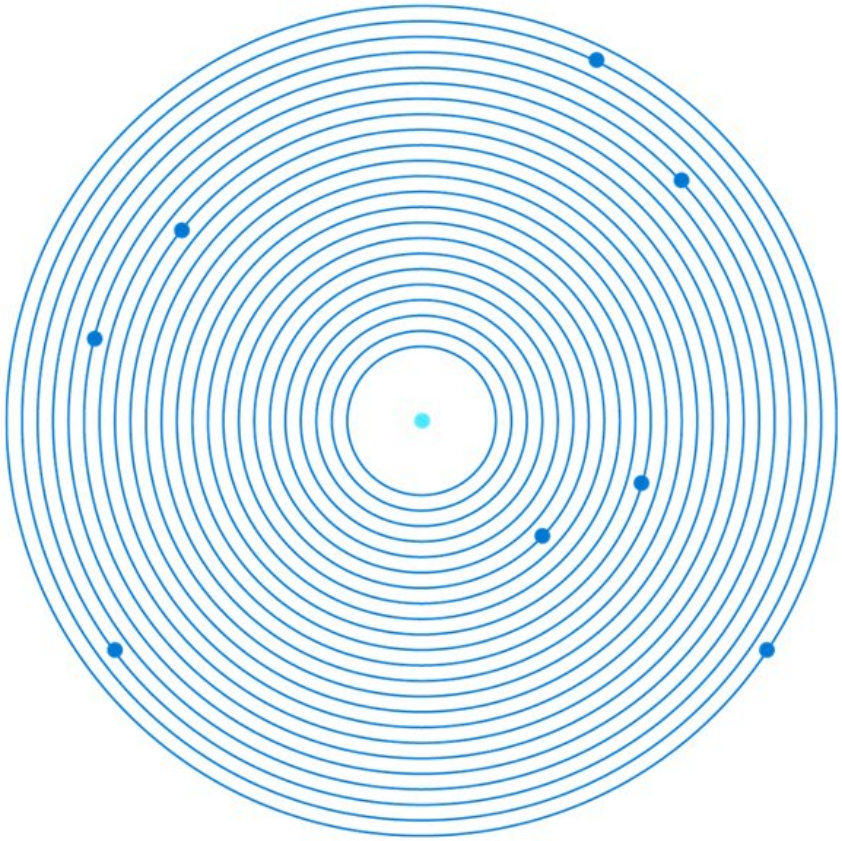
Provides everything you need to deploy your solution or serves as a starting point for your template



https://azure.microsoft.com/en-us/resources/templates/

Microsoft Azure

Module 04: Virtual Networking



Module Overview

Lesson 01: Virtual Networks

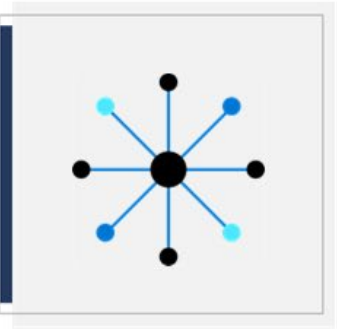
Lesson 02: IP Addressing

Lesson 03: Network Security Groups

Lesson 04: Azure Firewall

Lesson 05: Azure DNS

Lesson 01: Virtual Networks



Virtual Networks Overview

Azure Networking Components

Virtual Networks

Subnets

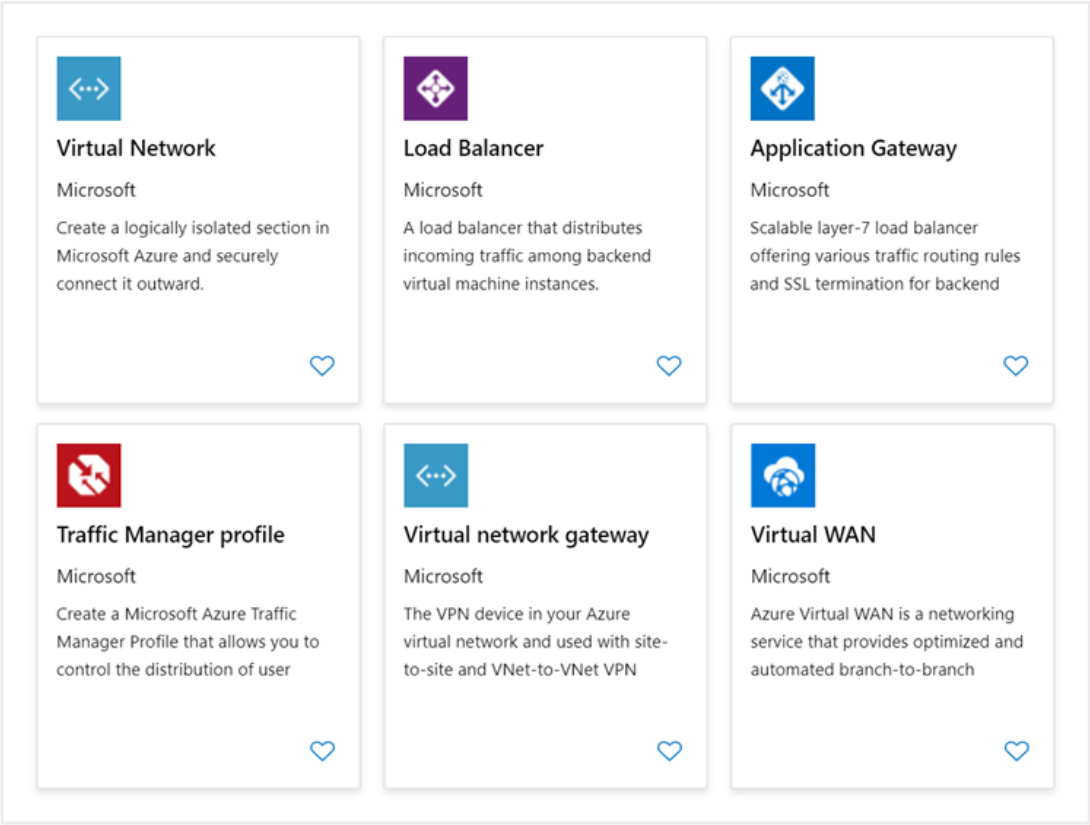
Implementing Virtual Networks

Azure Networking Components

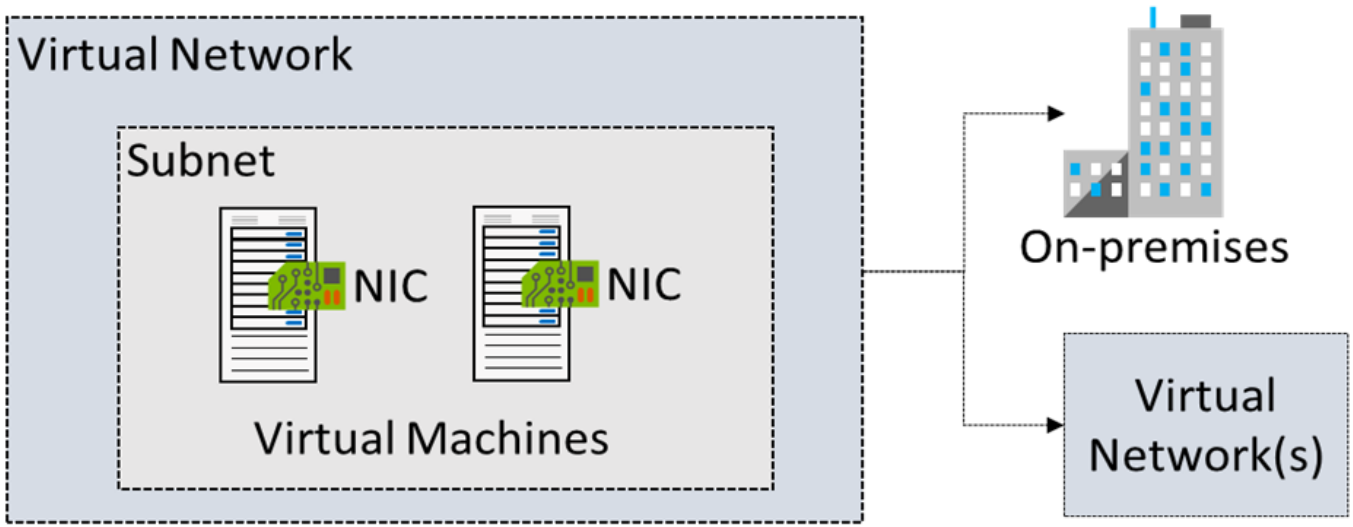
Adopting cloud solutions can save time and simplify operations

Azure requires the same types of networking functionality as on-premises infrastructure

Azure networking offers a wide range of services and products



Virtual Networks



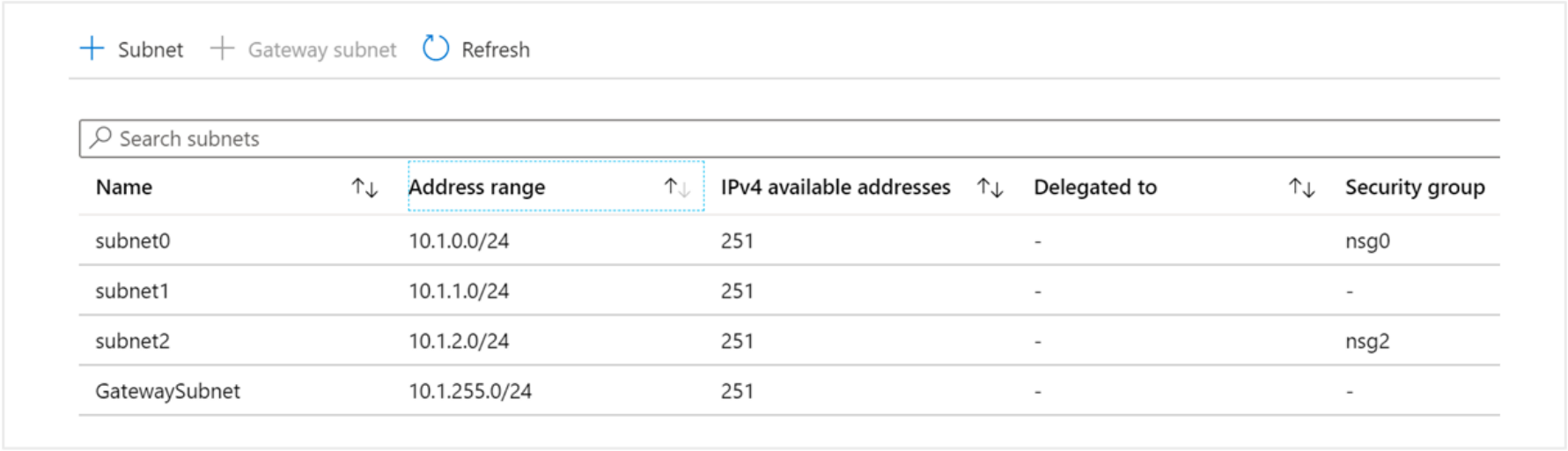
Logical representation of your own network

Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

Enable hybrid cloud scenarios

Subnets



A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Each subnet must have a unique address range – cannot overlap with other subnets in the virtual network in the subscription

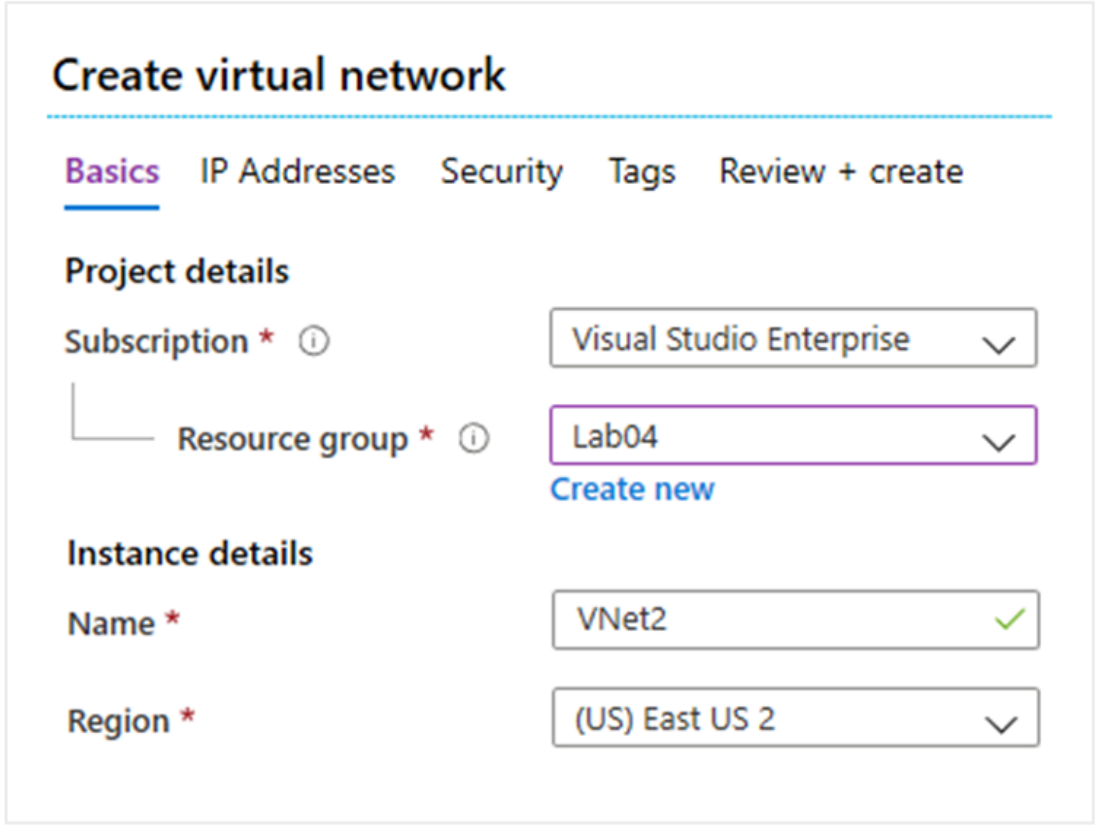
Implementing Virtual Networks

Create new virtual networks at any time

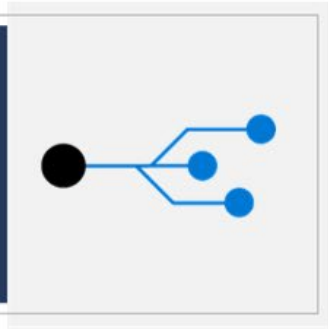
Add virtual networks when you create a virtual machine

Need to define the address space, and at least one subnet

Be careful with overlapping address spaces



Lesson 02: IP Addressing



IP Addressing Overview

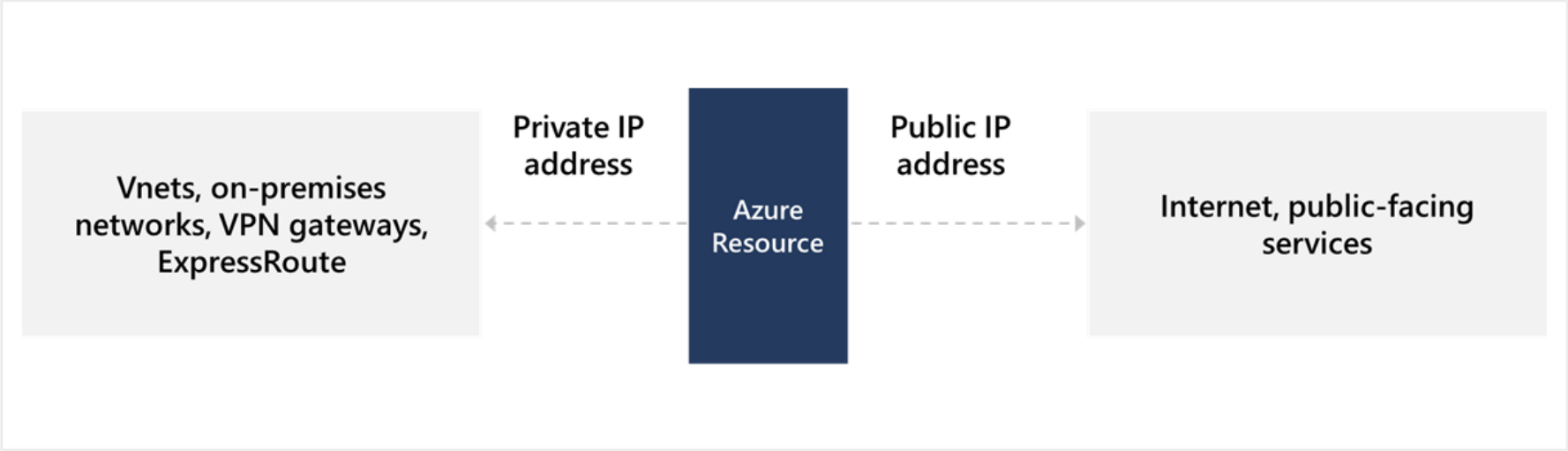
IP Addressing

Creating IP Addresses

Public IP Addresses

Private IP Addresses

IP Addressing



Private IP addresses - used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

Public IP addresses - used for communication with the Internet, including Azure public-facing services

Creating Public IP Addresses

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Available in Dynamic, Static or both (depending on SKU):

Zone redundant

Not mixable or immutable

Range of contiguous addresses available as a prefix

Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	No
Application Gateway	Front-end configuration	Yes	Yes*

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

Dynamic (default). Azure assigns the next available unassigned or unreserved IP address in the subnet's address range

Static. You select and assign any unassigned or unreserved IP address in the subnet's address range

Lesson 03: Network Security Groups

Network Security Groups Overview

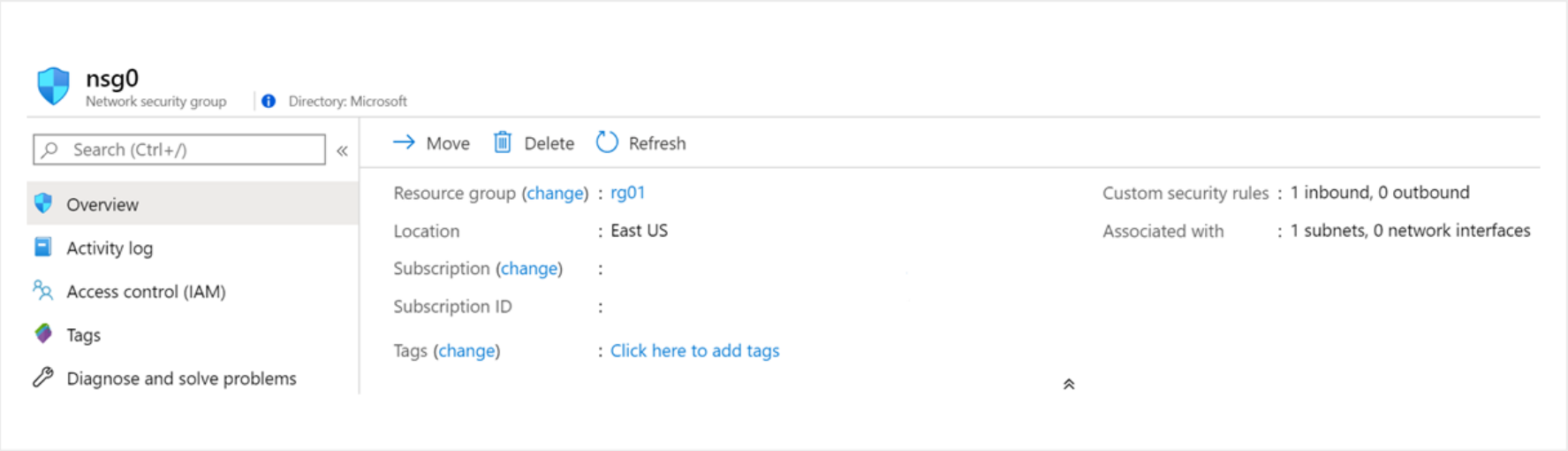
Network Security Groups (NSG)

NSG Rules

NSG Effective Rules

Creating NSG Rules

Network Security Groups



Limit network traffic to resources in a virtual network

Contains a list of security rules that allow or deny inbound or outbound network traffic

Can be associated to a subnet or a network interface

NSG Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ RDP_Inbound	3389	Any	Any	Any	✔ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✔ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✖ Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✔ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✖ Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

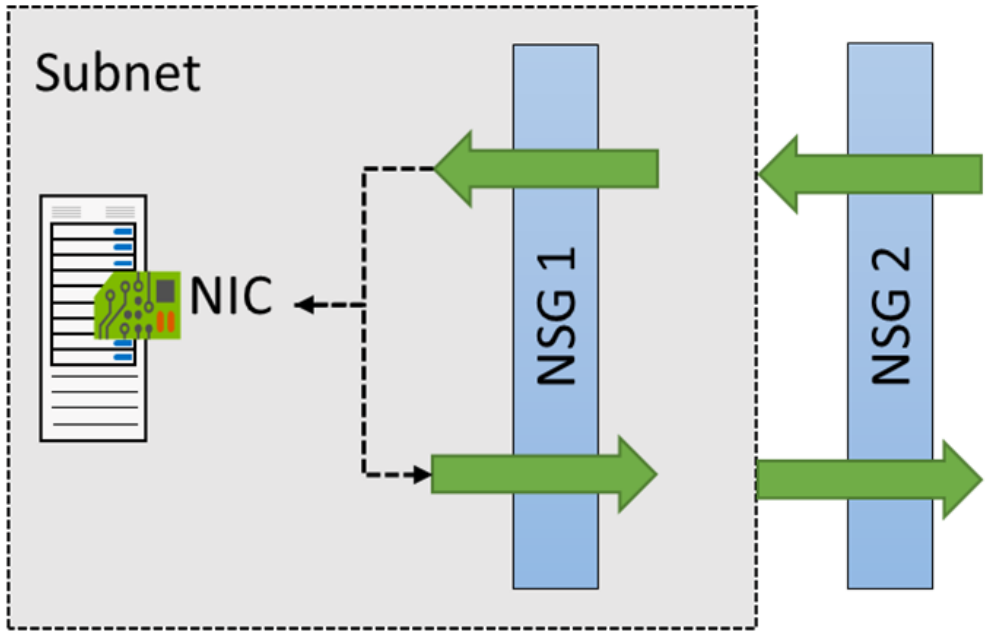
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

NSG Effective Rules

NSGs are evaluated independently for the subnet and NIC

An “allow” rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied



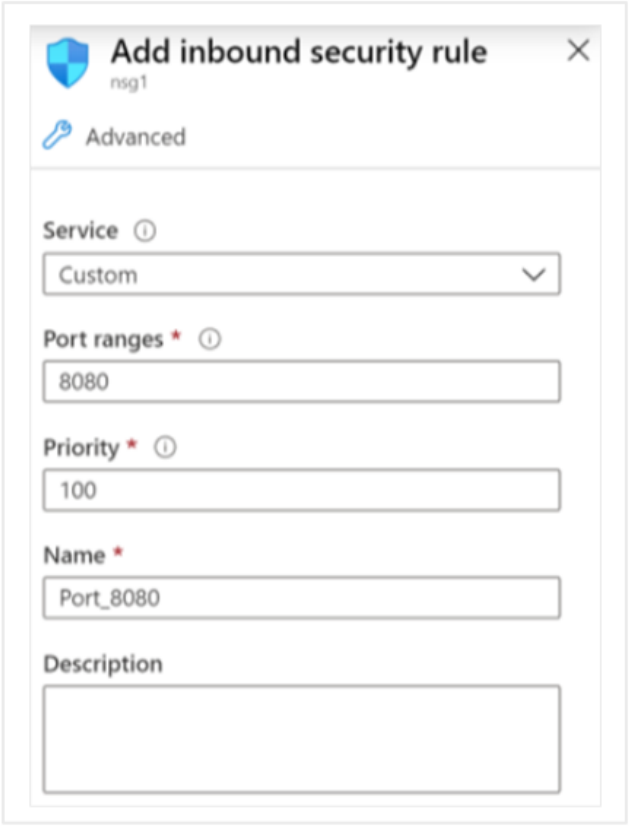
Creating NSG rules

Select from a large variety of services

Service – The destination protocol and port range for this rule

Port ranges – Single port or multiple ports

Priority – The lower the number, the higher the priority

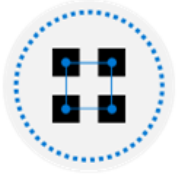


Lesson 04: Azure Firewall

Azure Firewall Overview

Azure Firewall

Implementing Firewalls



Firewall Rules

Azure Firewall

Stateful firewall as a service

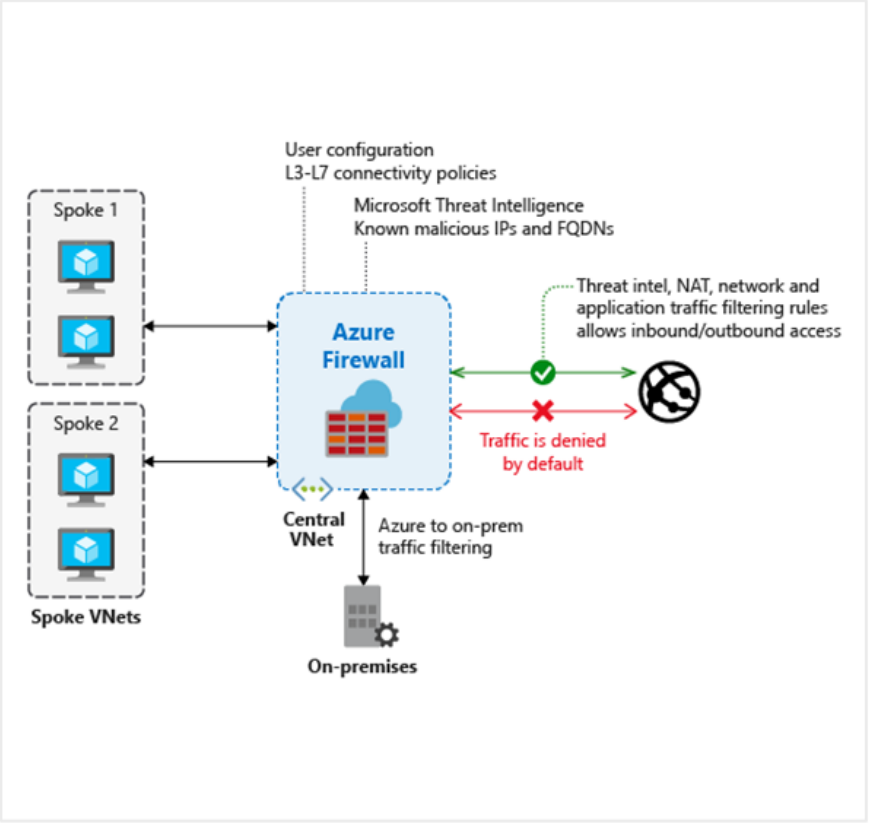
Built-in high availability with unrestricted cloud scalability

Create, enforce, and log application and network connectivity policies

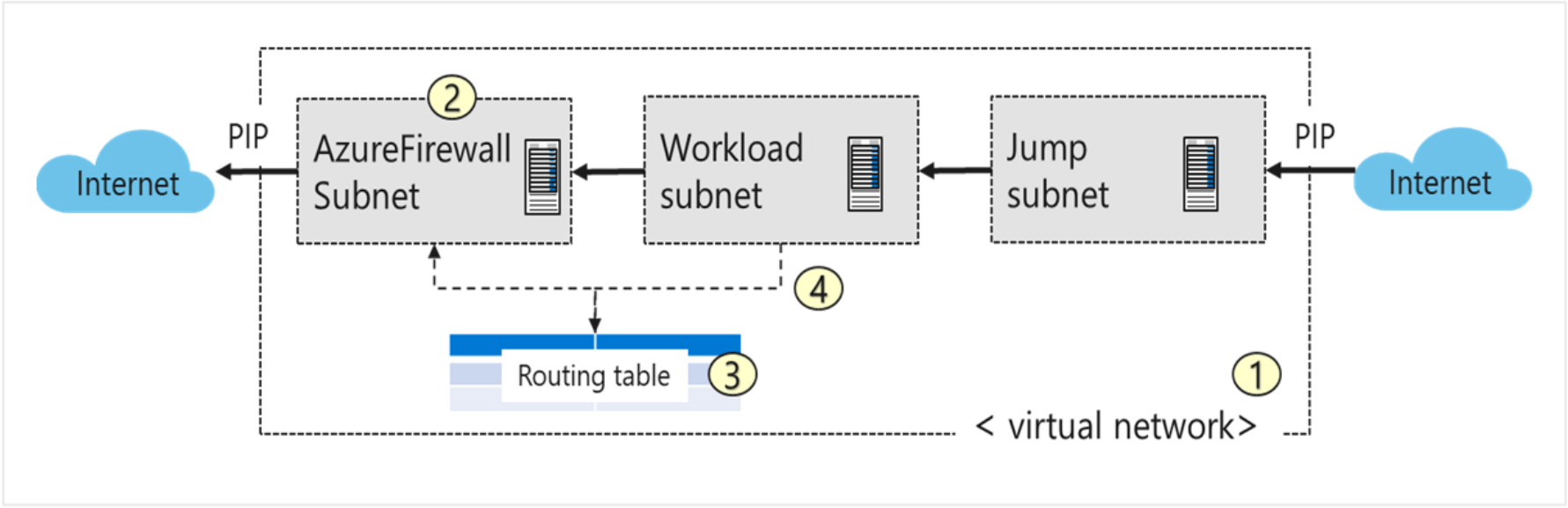
Threat intelligence-based filtering

Fully integrated with Azure Monitor for logging and analytics

Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways



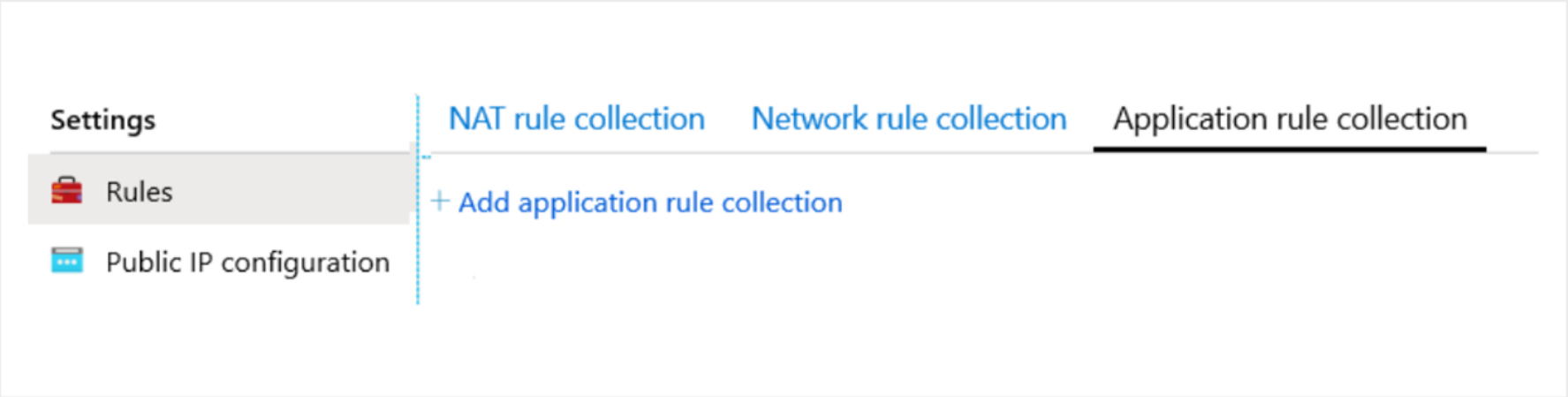
Implementing Firewalls



1. Create the network infrastructure
2. Deploy the firewall
3. Create a default route
4. Configure rules

✓ **In production deployments, a Hub and Spoke model is recommended.**

Firewall Rules



NAT rules. Configure DNAT rules to allow incoming connections

Network rules. Configure rules that contain source addresses, protocols, destination ports, and destination addresses

Application rules. Configure fully qualified domain names (FQDNs) that can be accessed from a subnet

Lesson 05: Azure DNS

Azure DNS Overview

Domains and Custom Domains

Verifying Custom Domain Names

Azure DNS Zones

DNS Delegation

DNS Record Sets

DNS for Private Domains

Private Zones Scenarios

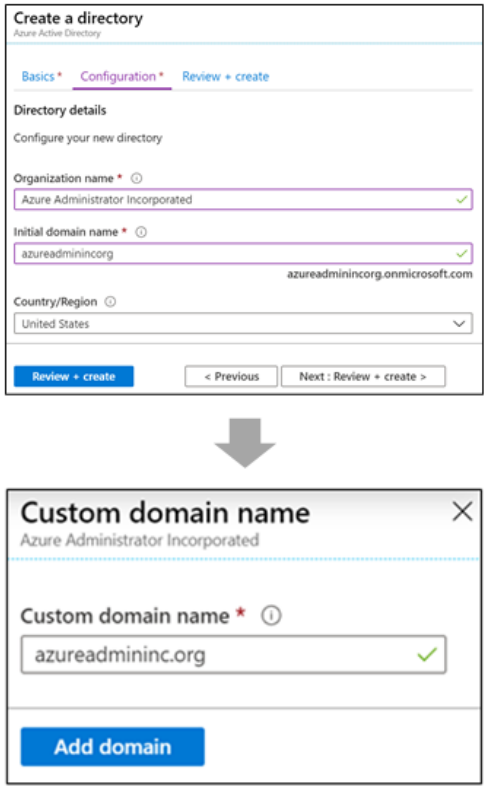
Domains and Custom Domains

When you create an Azure subscription an Azure AD domain is created for you

The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can customize/change the name

After the custom name is added it must be verified (next topic)



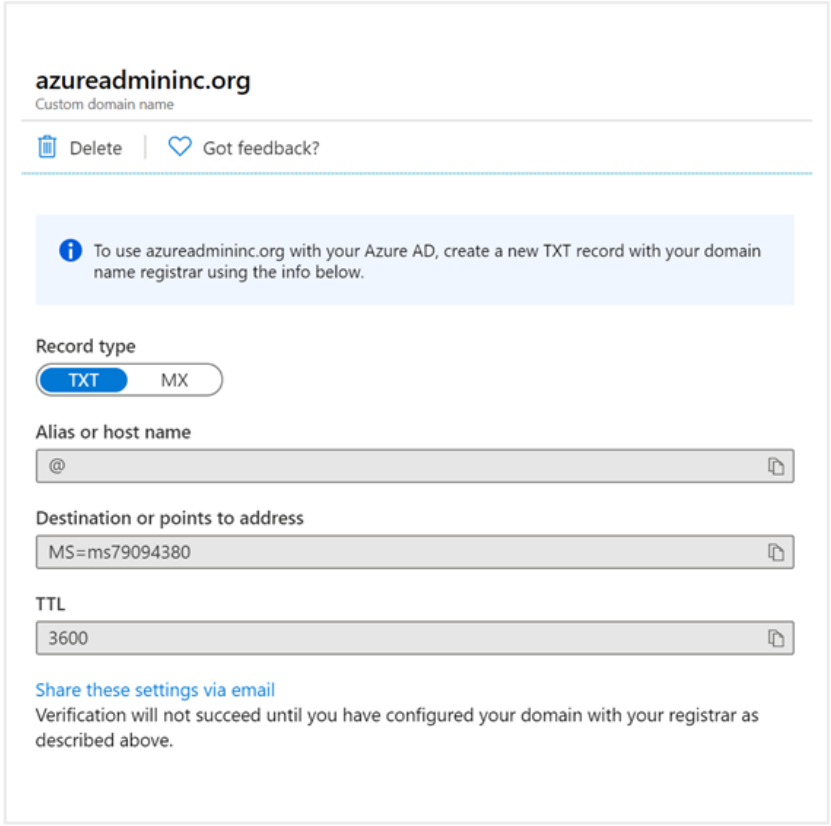
Verify the Custom Domain Name

Verification demonstrates ownership of the domain name

Add a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone

Azure will query the DNS domain for the presence of the record

This could take several minutes or several hours



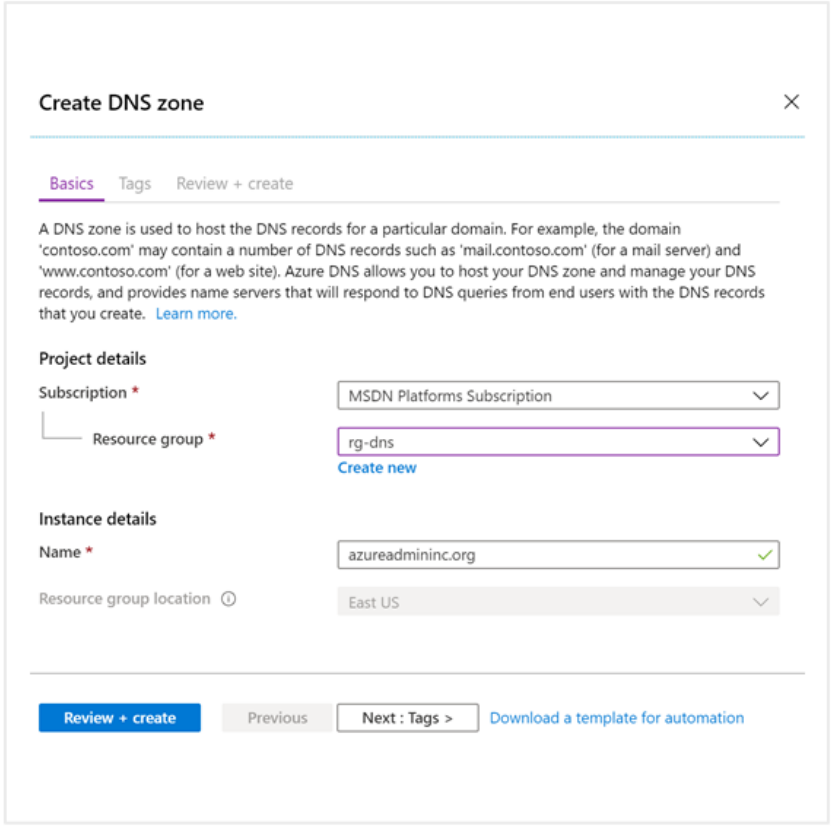
Azure DNS Zones

A DNS zone hosts the DNS records for a domain

The name of the zone must be unique within the resource group

Where multiple zones share the same name, each instance is assigned different name server addresses

Root/Parent domain is registered at the registrar and pointed to Azure NS

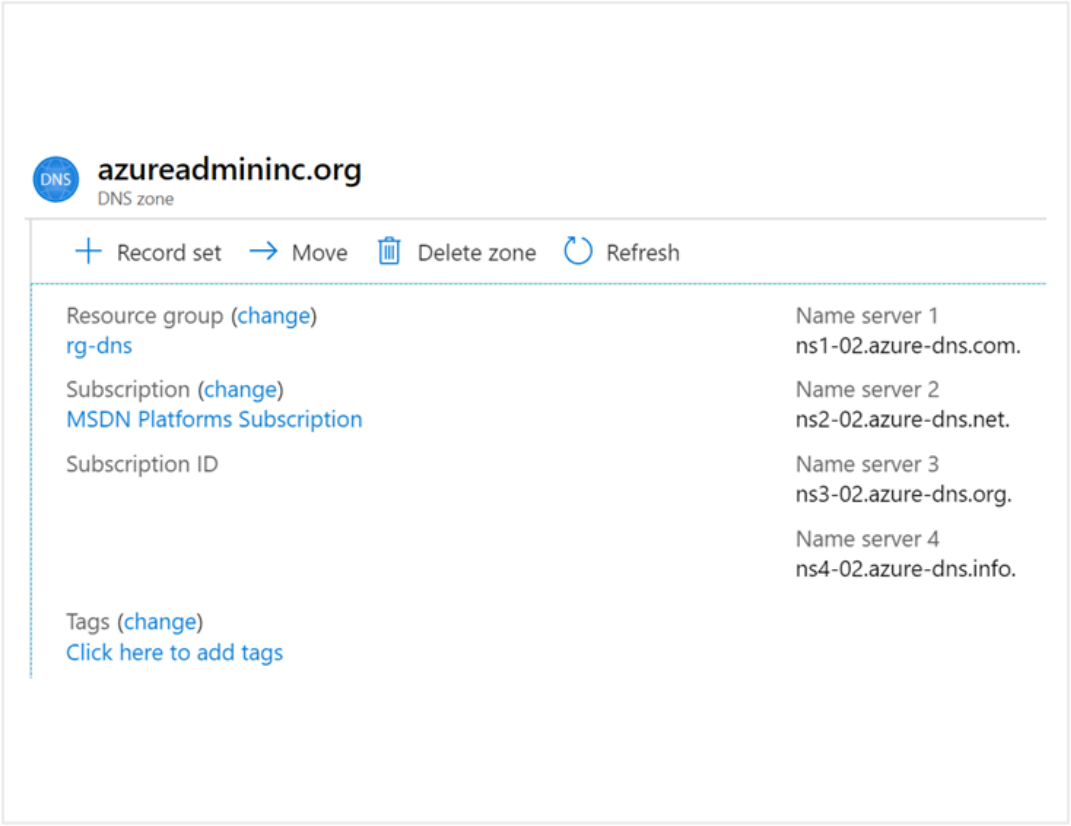


DNS Delegation

When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four

Once the DNS zone is created, update the parent registrar

For child zones, register the NS records in the parent domain



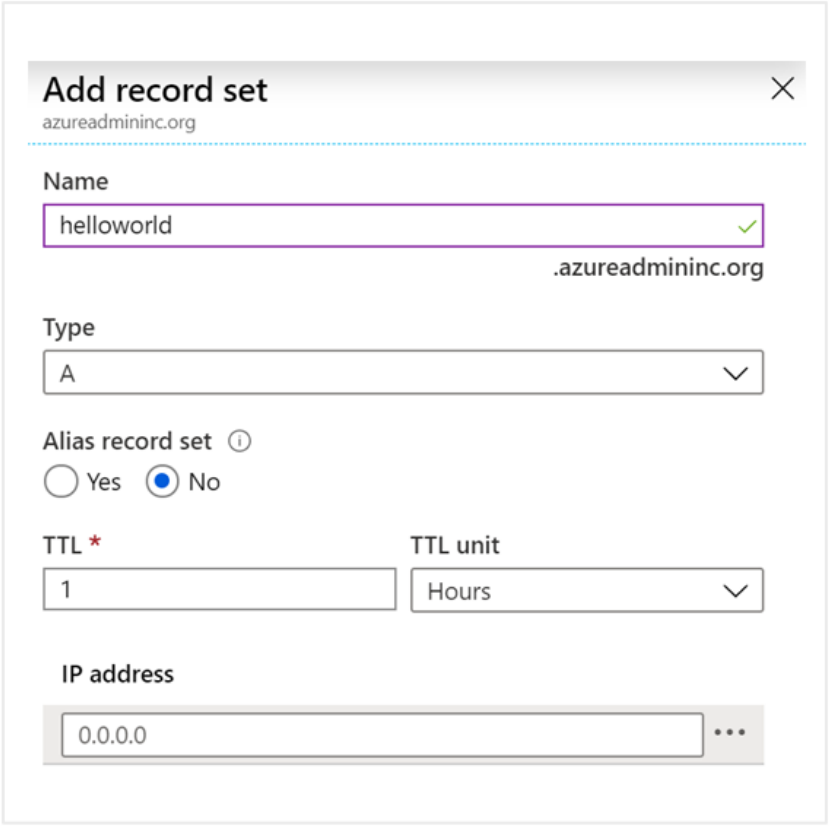
DNS Record Sets

A record set is a collection of records in a zone that have the same name and are the same type

You can add up to 20 records to any record set

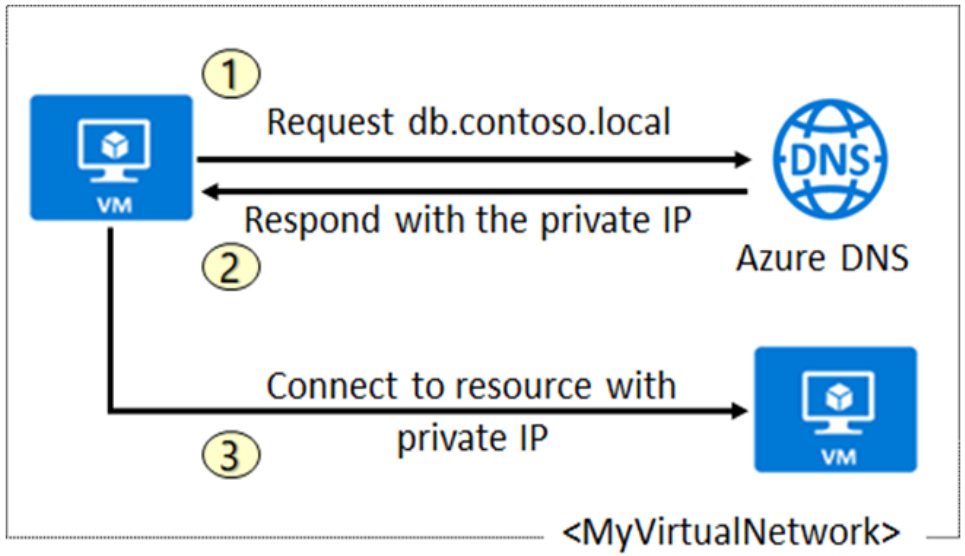
A record set cannot contain two identical records

Changing the drop-down Type, changes the information required

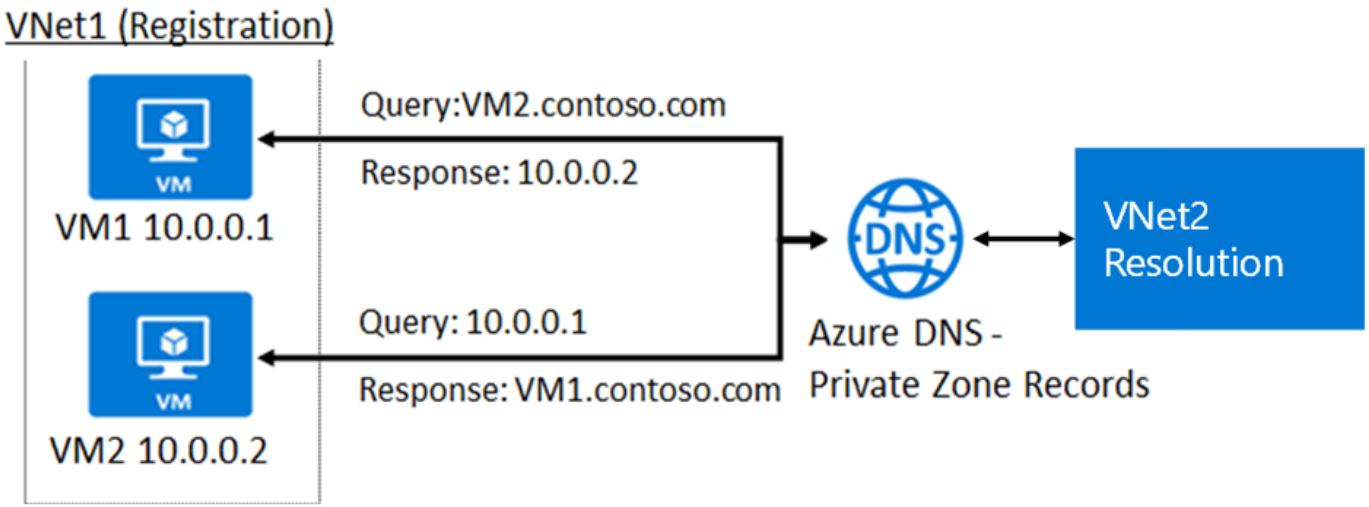


DNS for Private Domains

- Use your own custom domain names
- Provides name resolution for VMs within a VNet and between VNets
- Automatic hostname record management
- Removes the need for custom DNS solutions
- Use all common DNS records types
- Available in all Azure regions



Private Zone Scenarios



DNS resolution in VNet1 is private and not accessible from the Internet

DNS queries across the virtual networks are resolved

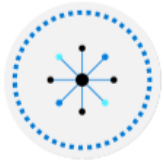
Reverse DNS queries are scoped to the same virtual network

Microsoft Azure

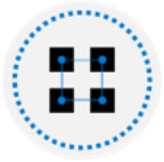
Module 05:
Intersite Connectivity

Module Overview

Lesson 01: VNet Peering

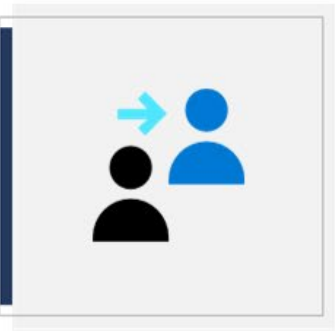


Lesson 02: VPN Gateway Connections

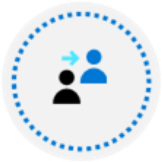


Lesson 03: ExpressRoute and Virtual WAN

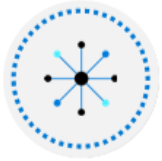
Lesson 01: VNet Peering



VNet Peering Overview



VNet Peering



Gateway Transit and Connectivity

Configure VNet Peering

Service Chaining

VNet Peering

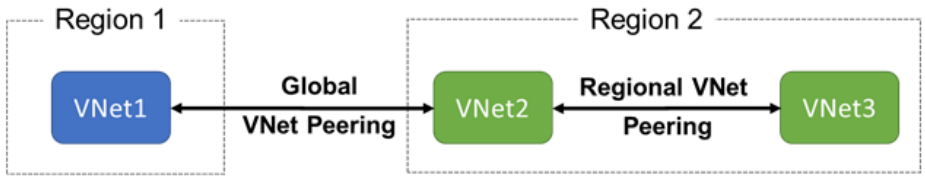
VNet peering connects two Azure virtual networks

Two types of peering: Regional and Global

Peered networks use the Azure backbone for privacy and isolation

You can peer across subscriptions

Easy to setup, seamless data transfer, and great performance

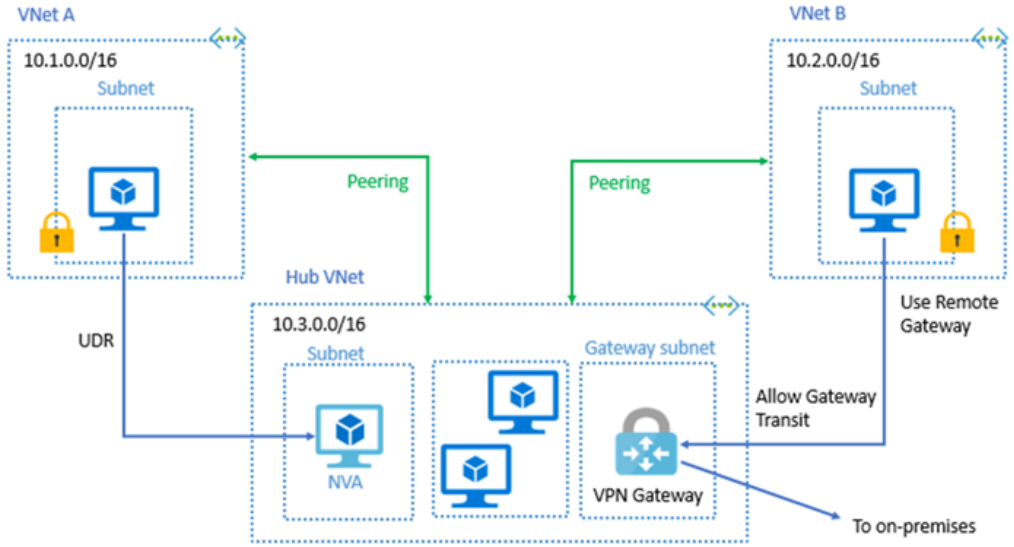


Gateway Transit and Connectivity

Gateway transit allows peered virtual networks to share the gateway and get access to resources

No VPN gateway is required in the peered virtual network

Default VNet peering provides full connectivity



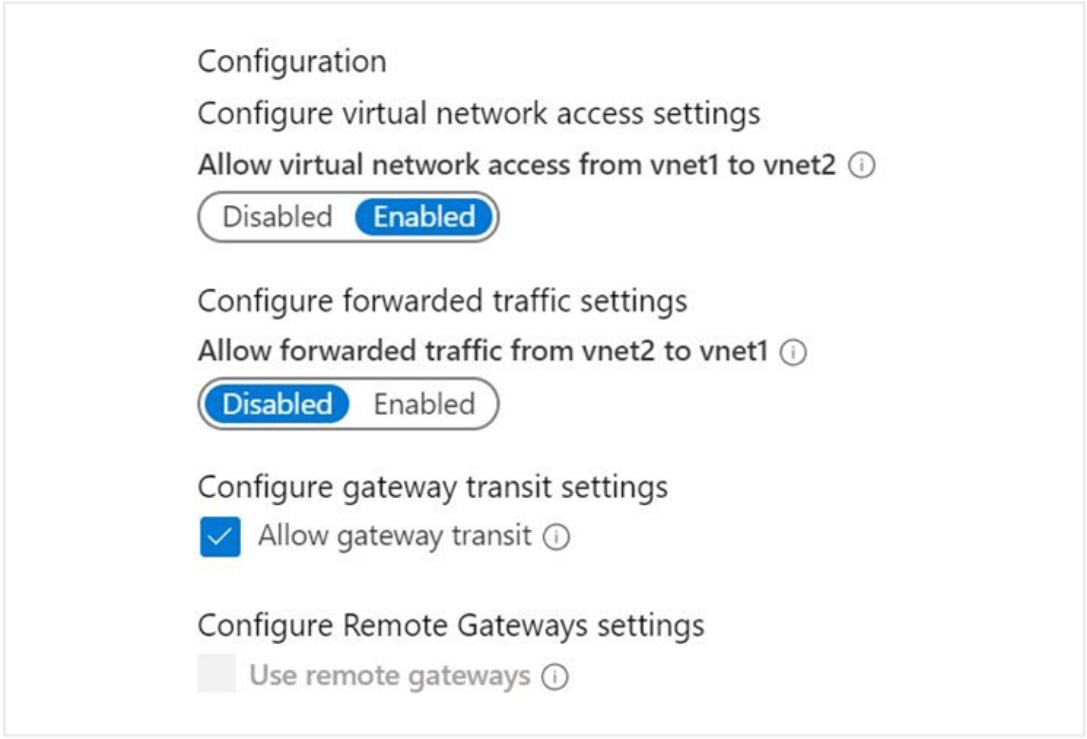
✓ IP address spaces of connected networks can't overlap

Configure VNet Peering

Allow forwarded traffic – From within the peer virtual network into your virtual network

Allow gateway transit – Allows the peer virtual network to use your virtual network gateway

Use remote gateways – Allows the virtual network to use another virtual network's gateway



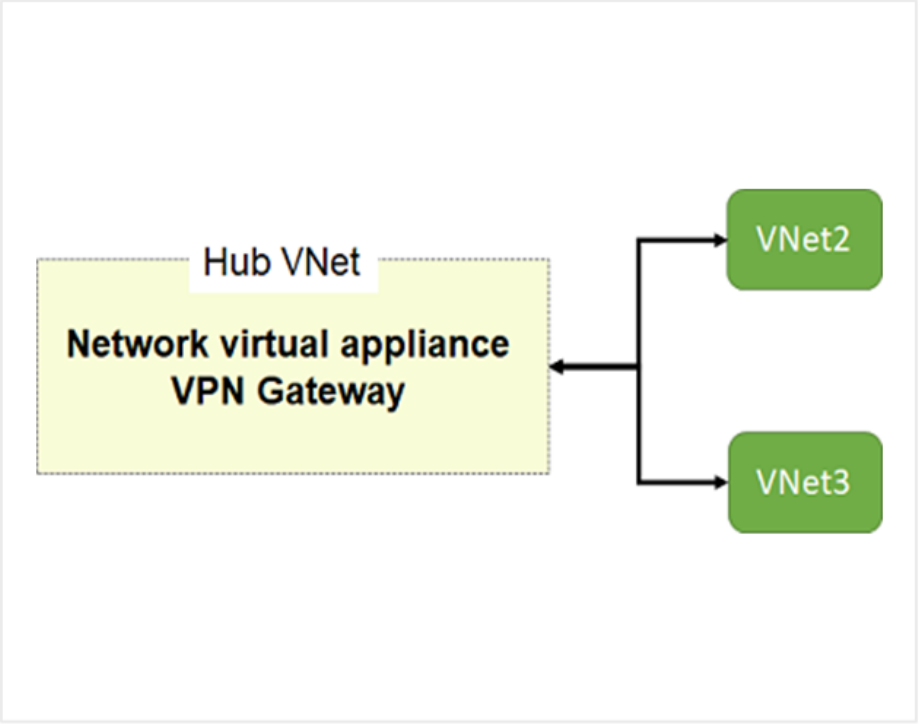
✓ **If you select 'Allow gateway transit' on one virtual network; then you should select 'Use remote gateways' on the other virtual network**

Service Chaining

Leverage user-defined routes and service chaining to implement custom routing

Implement a VNet hub with a network virtual appliance or a VPN gateway

Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes



Lesson 02: VPN Gateway Connections

VPN Gateway Connections Overview

VPN Gateways

Implement Site-to-Site VPN Connections

Create the Gateway Subnet

VPN Gateway Configuration

VPN Gateway Types

VPN Gateway SKU and Generation

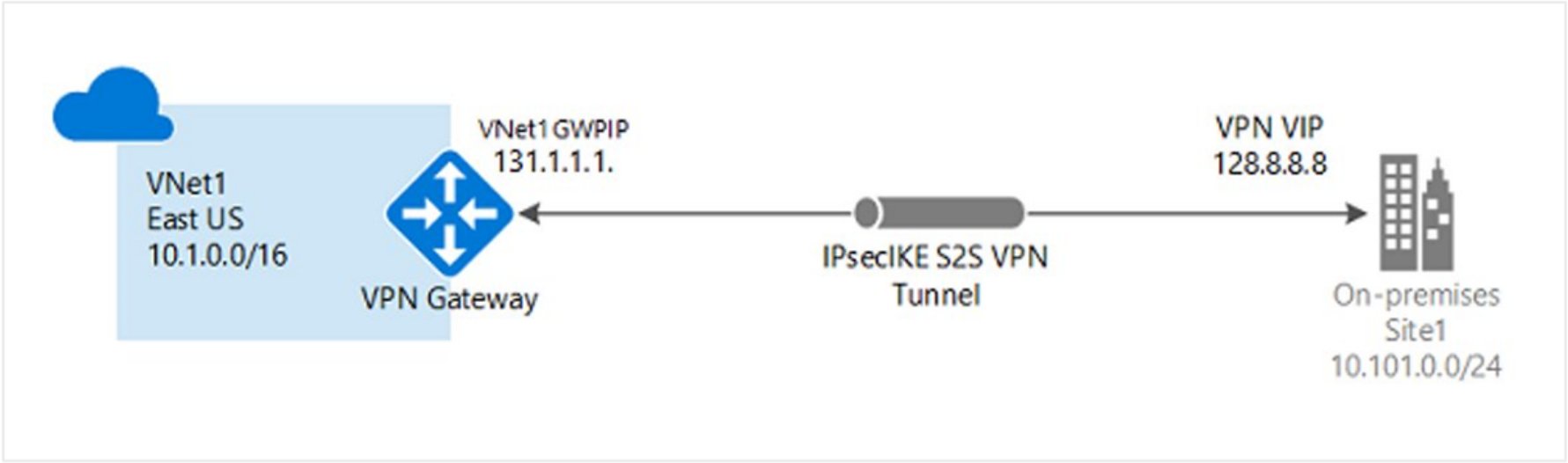
Create the Local Network Gateway

Configure the On-premises VPN Device

Create the VPN Connection

High Availability Scenarios

VPN Gateways

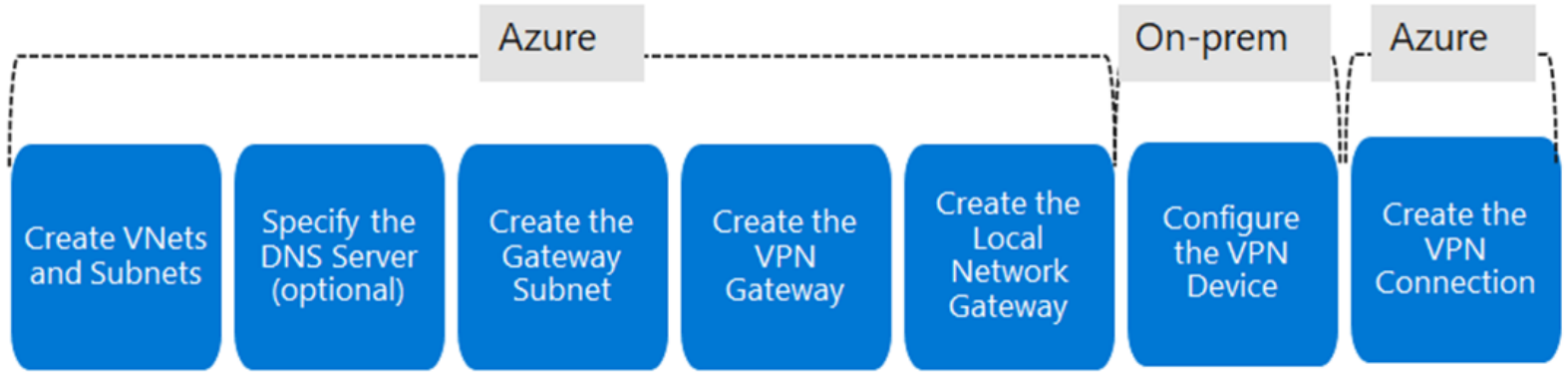


Site-to-site connections connect on-premises datacenters to Azure virtual networks

Network-to-network connections connect Azure virtual networks (custom)

Point-to-site (User VPN) connections connect individual devices to Azure virtual networks

Implement Site-to-Site VPN Connections



Take time to carefully plan your network configuration

The on-premises part is necessary only if you are configuring Site-to-Site

Always verify and test your connections

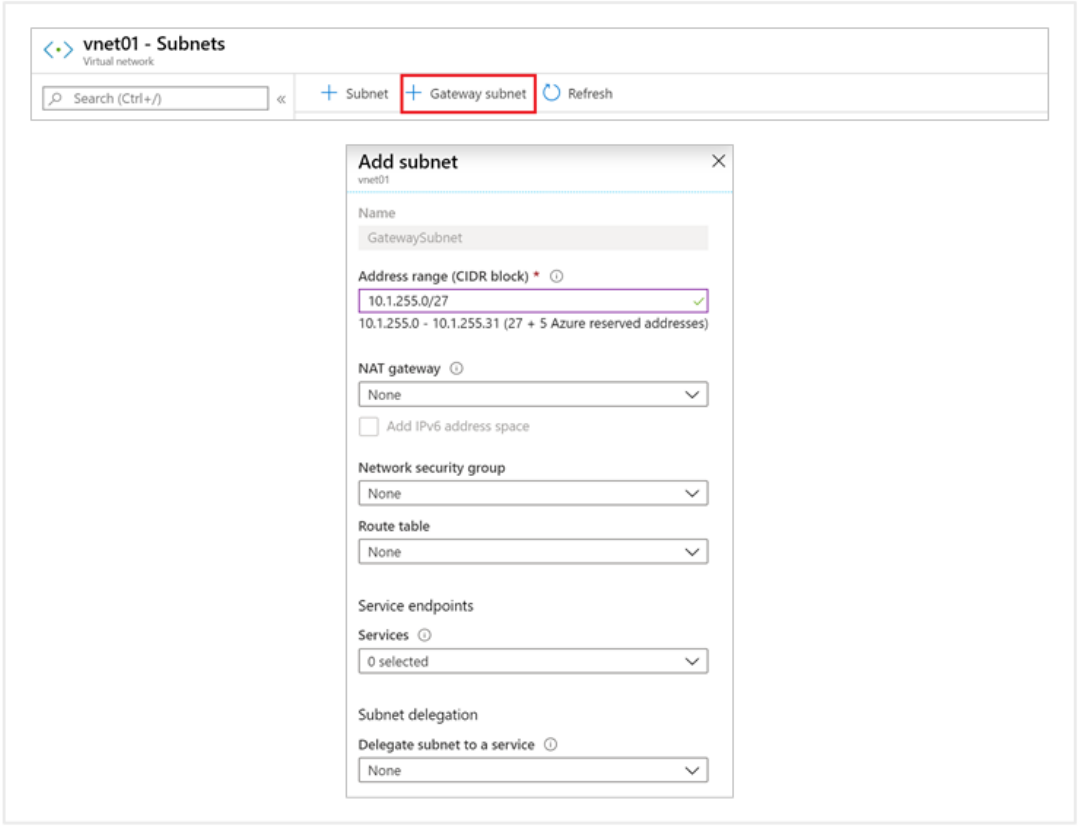
Create the Gateway Subnet

The gateway subnet contains the IP addresses; if possible, use a CIDR block of /28 or /27

When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings

Never deploy other resources (for example, additional VMs) to the gateway subnet

Avoid associating a NSG with the gateway subnet



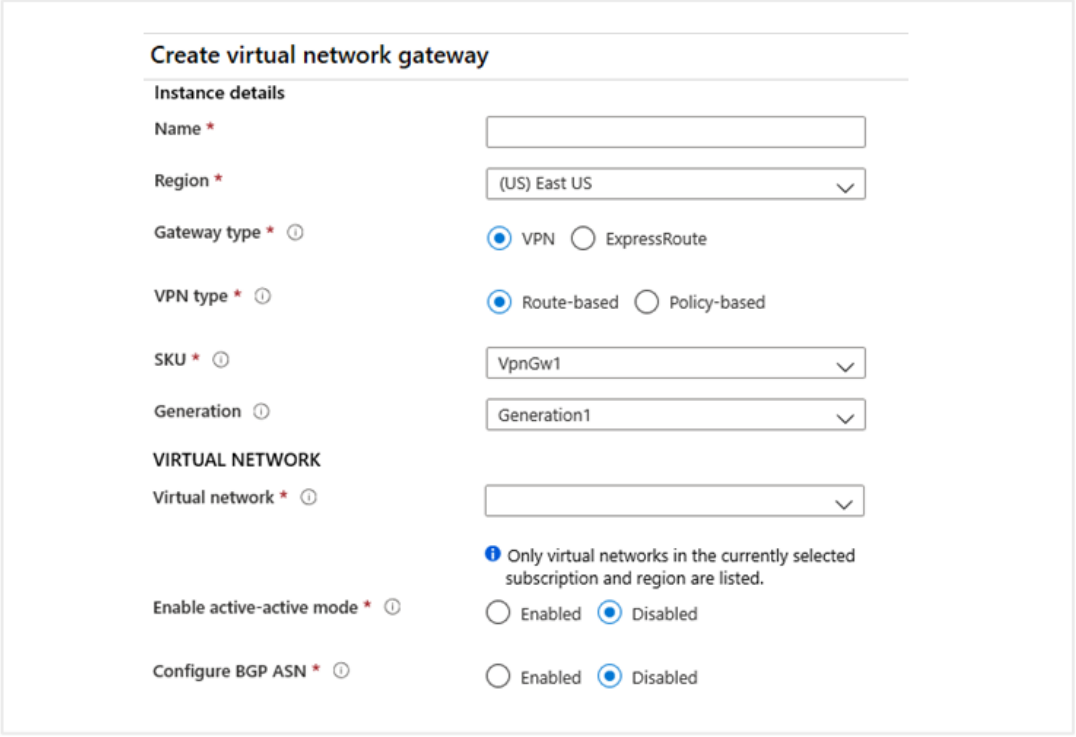
VPN Gateway Configuration

Most VPN types are Route-based

Your choice of gateway SKU affects the number of connections you can have and the aggregate throughput benchmark

Associate a virtual network that includes the gateway subnet

The gateway needs a public IP address



✓ It can take up to 45 minutes to provision the VPN gateway

VPN Gateway Types

Route-based VPNs use routes in the IP forwarding or routing table to direct packets:

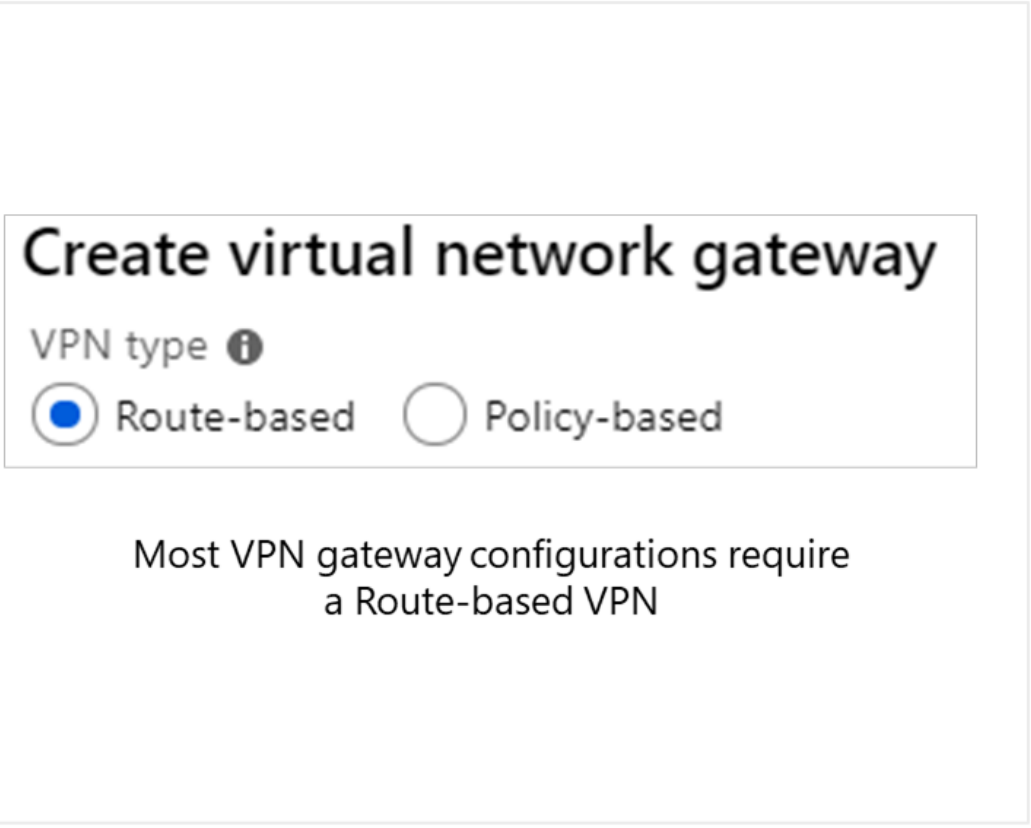
Supports for IKEv2

Can use dynamic routing protocols

Policy-based VPNs encrypt and direct packets through IPsec tunnels based on the IPsec policies:

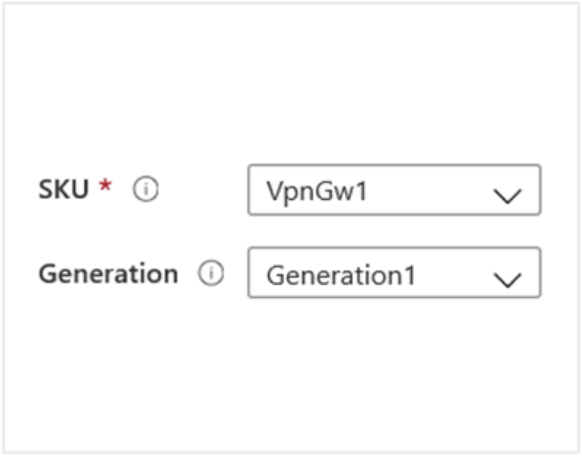
Support for IKEv1 only

Legacy on-premises VPN devices



Most VPN gateway configurations require a Route-based VPN

Gateway SKU and Generation



Sampling of available SKUs

Gen	SKU	S2S/VNet-to-VNet Tunnels	P2S IKEv2 Connections	Throughput Benchmark
1	VpnGw1/Az	Max. 30	Max. 250	650 Mbps
1	VpnGw2/Az	Max. 30	Max. 500	1.0 Gbps
2	VpnGw2/Az	Max. 30	Max. 500	1.25 Gbps
1	VpnGw3/Az	Max. 30	Max. 1000	1.25 Gbps
2	VpnGw3/Az	Max. 30	Max. 1000	2.5 Gbps
2	VpnGw4/Az	Max. 30	Max. 5000	5.0 Gbps

The Gateway SKU affects the connections and the throughput

Resizing is allowed within the generation

The Basic SKU (not shown) is legacy and should not be used

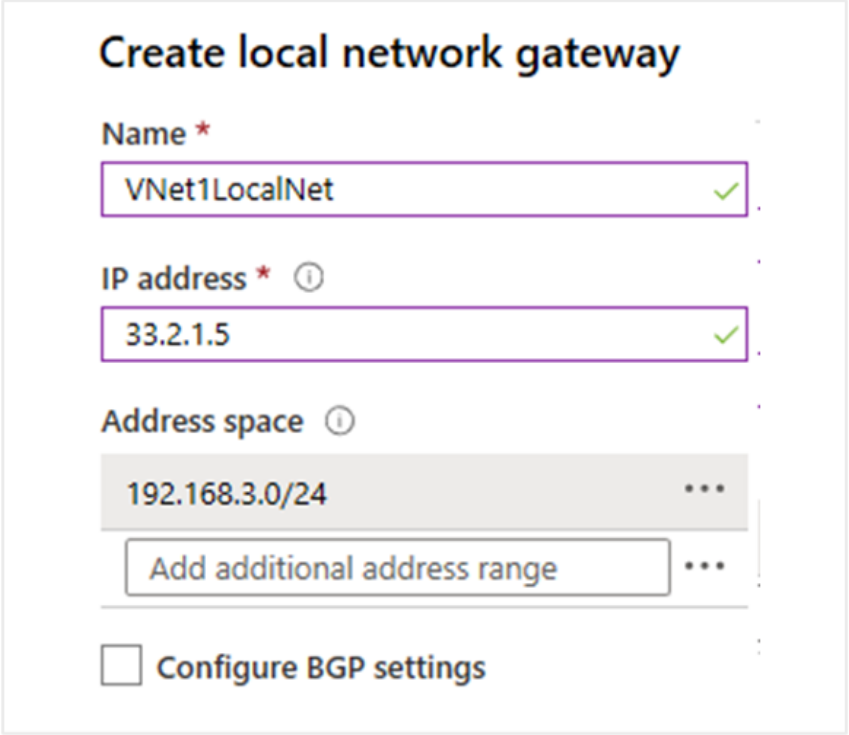
Create the Local Network Gateway

Defines the on-premises network configuration

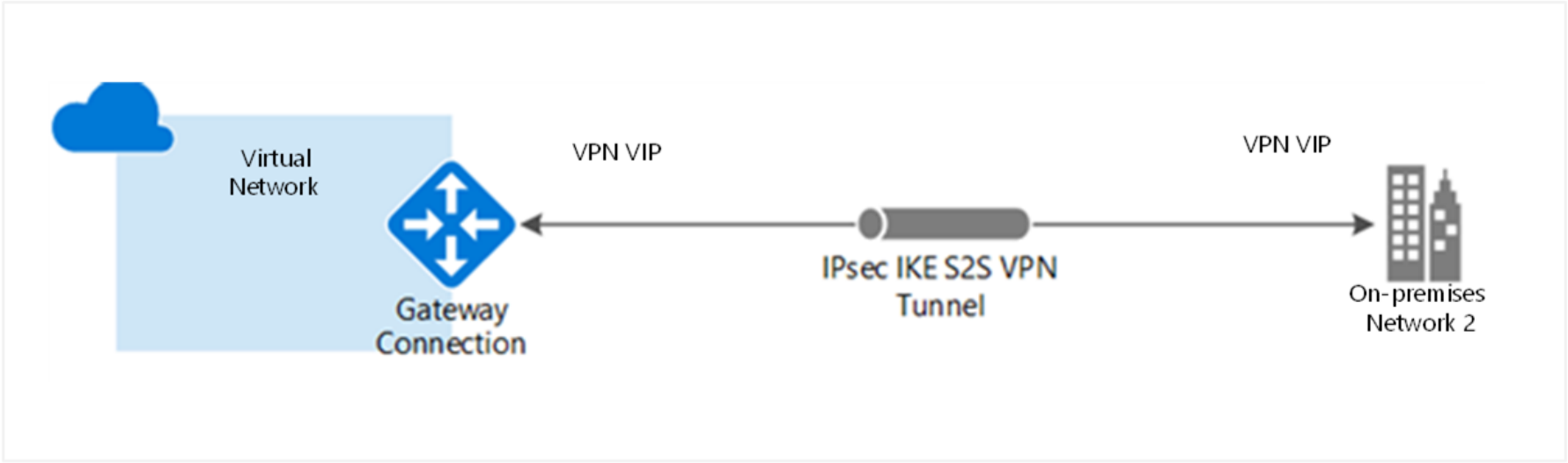
Give the site a name by which Azure can refer to it

The local gateway needs a public IP address

Specify the IP address prefixes that will be routed through the gateway to the VPN device



Configure the On-premises VPN Device



Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)	A VPN device configuration script may be available	Remember the shared key for the Azure connection (next step)	Specify the public IP address (previous step)

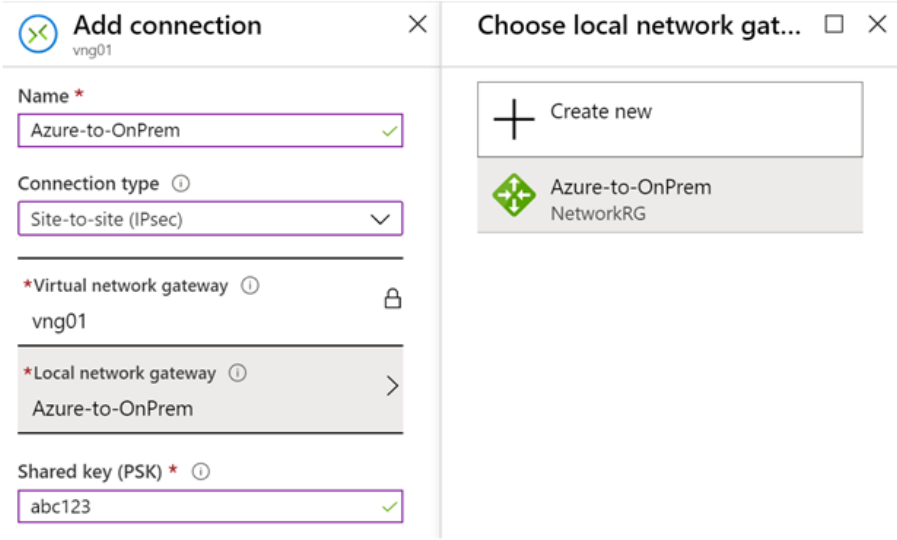
Create the VPN Connection

Once your VPN gateways is created and the on-premises device is configured, create a connection object

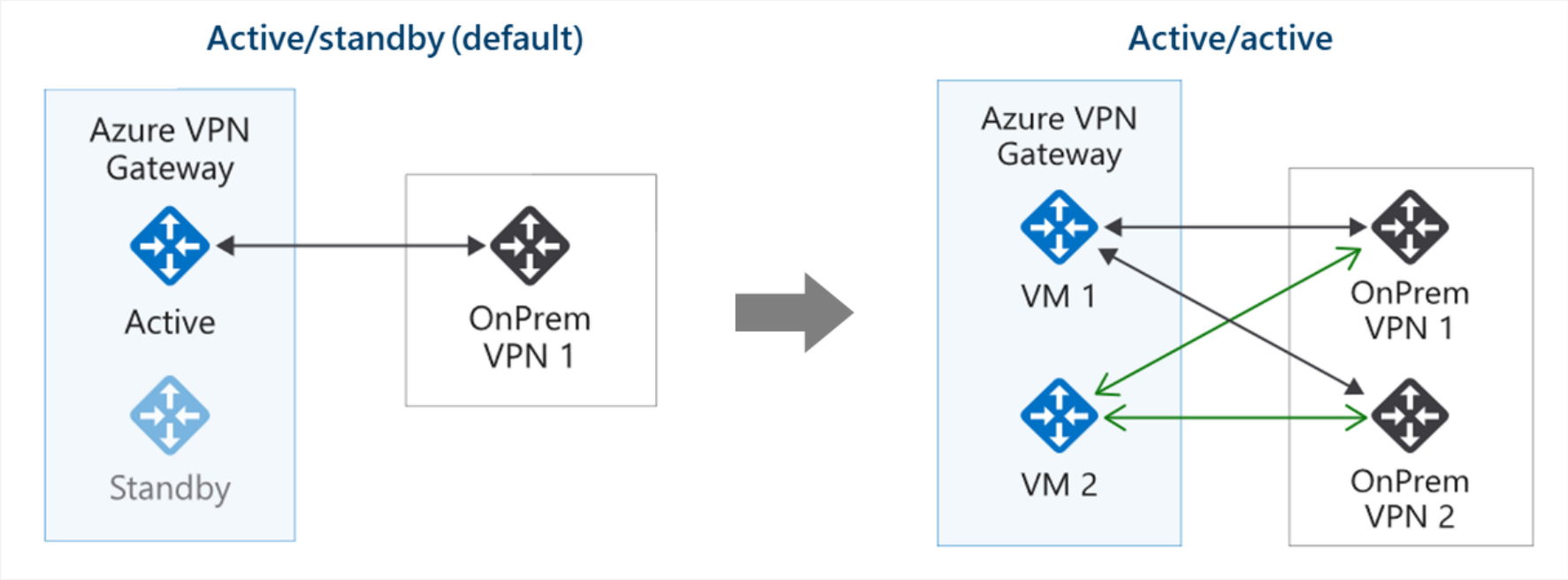
Configure a name for the connection and specify the type as Site-to-site (IPsec)

Select the VPN gateway and the Local Network Gateway

Enter the Shared key for the connection



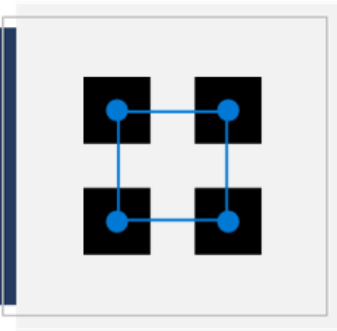
High Availability Scenarios



VPN gateways are deployed as two instances

Enable **active/active mode** for higher availability

Lesson 03: ExpressRoute and Virtual WAN



ExpressRoute and Virtual WAN Overview

ExpressRoute

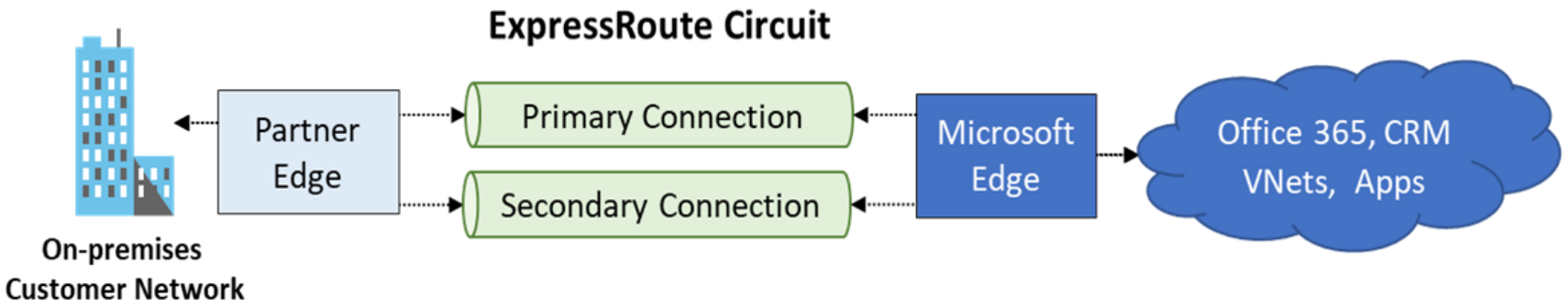
ExpressRoute Capabilities

Coexisting Site-to-Site and ExpressRoute

Intersite Connection Comparisons

Virtual WANs

ExpressRoute



Private connections between your on-premises network and Microsoft datacenters

Connections do not go over the public Internet – Partner network

Secure, reliable, low latency, high speed connections

ExpressRoute Capabilities

Layer 3 connectivity with redundancy

Connectivity to all regions within a geography

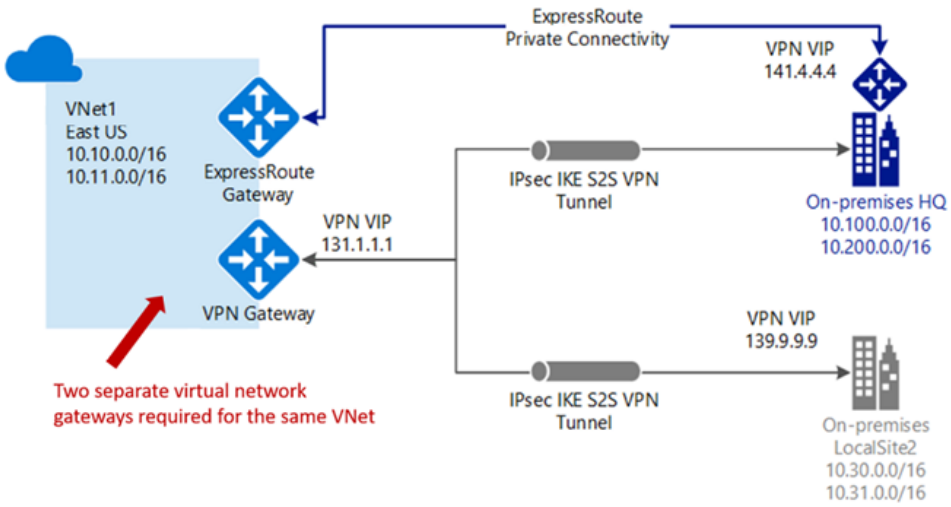
Global connectivity with ExpressRoute premium add-on

Across on-premises connectivity with ExpressRoute Global Reach

Bandwidth options – 50 Mbps to 100 Gbps

Billing models – Unlimited, metered, premium

Coexisting Site-to-Site and ExpressRoute



Use S2S VPN as a secure failover path for ExpressRoute

Use S2S VPNs to connect to sites that are not connected with ExpressRoute

Notice two VNet gateways for the same virtual network

Intersite Connections Comparison

Connection	Azure services supported	Bandwidth	Protocols	Typical use case
Virtual network, point-to-site	Azure IaaS services, Azure Virtual Machines	Based on the gateway SKU	Active/passive	Dev, test, and lab environments for cloud services and virtual machines
Virtual network, site-to-site	Azure IaaS services, Azure Virtual Machines	Typically <1 Gbps aggregate	Active/passive Active/active	Dev, test, and lab environments. Small-scale production workloads and virtual machines
ExpressRoute	Azure IaaS and PaaS services, Microsoft Office 365 services	50 Mbps up to 100 Gbps	Active/active	Enterprise-class and mission-critical workloads. Big data solutions

Virtual WANs

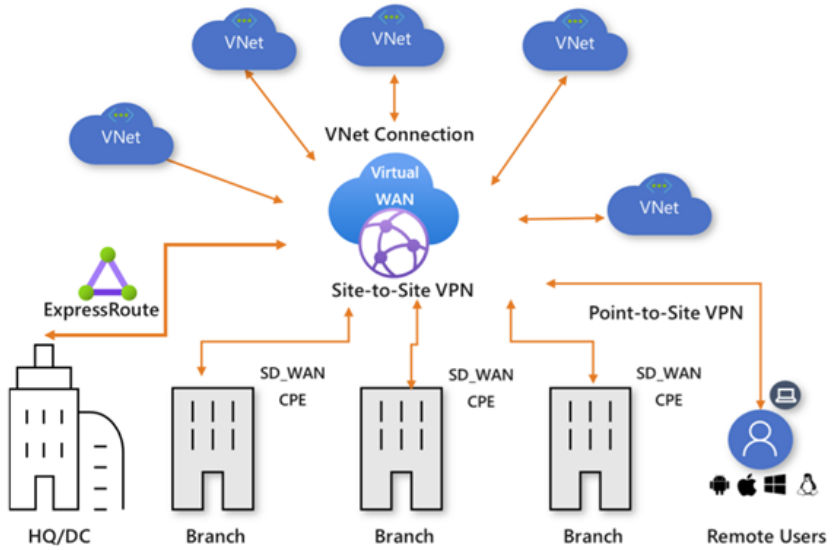
Brings together S2S, P2S, and ExpressRoute

Integrated connectivity using a hub-and-spoke connectivity model

Connect virtual networks and workloads to the Azure hub automatically

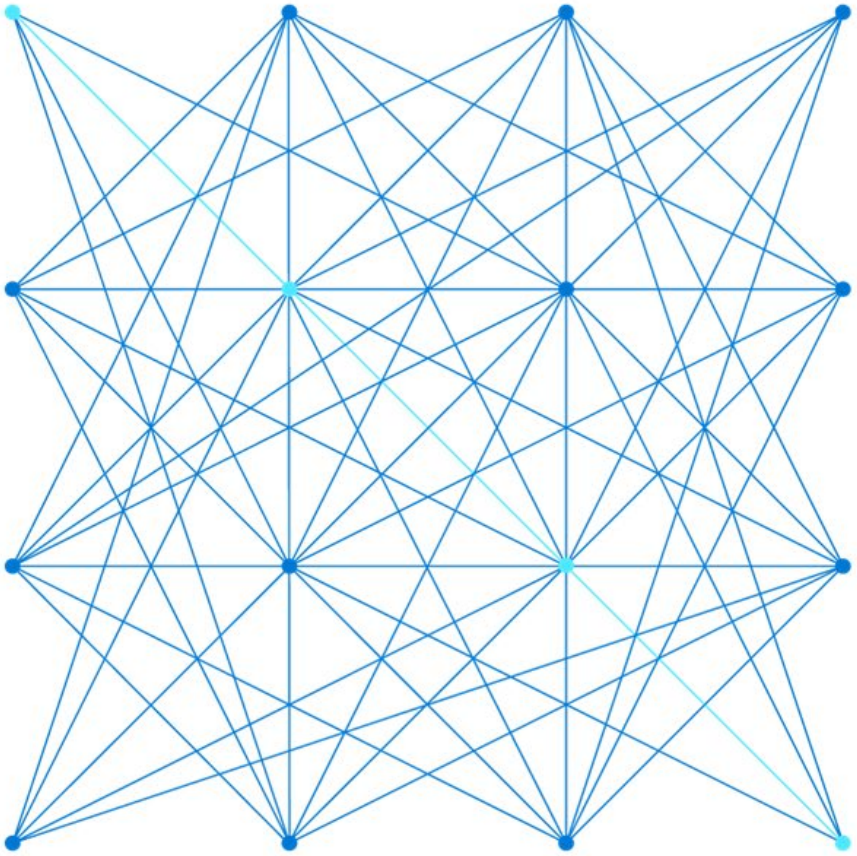
Visualize the end-to-end flow within Azure

Two types: Basic and Standard



Microsoft Azure

Module 06: Network Traffic Management



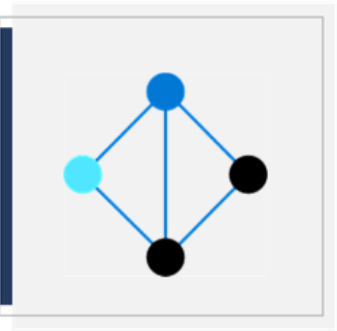
Module Overview

Lesson 01: Network Routing and Endpoints

Lesson 02: Azure Load Balancer

Lesson 03: Application Gateway

Lesson 01: Network Routing and Endpoints



Network Routing and Endpoints Overview

System Routes

User Defined Routes

Routing Example

Create a Routing Table

Create a Custom Route

Associate the Route Table

Demonstration – Custom Routing tables

Service Endpoints

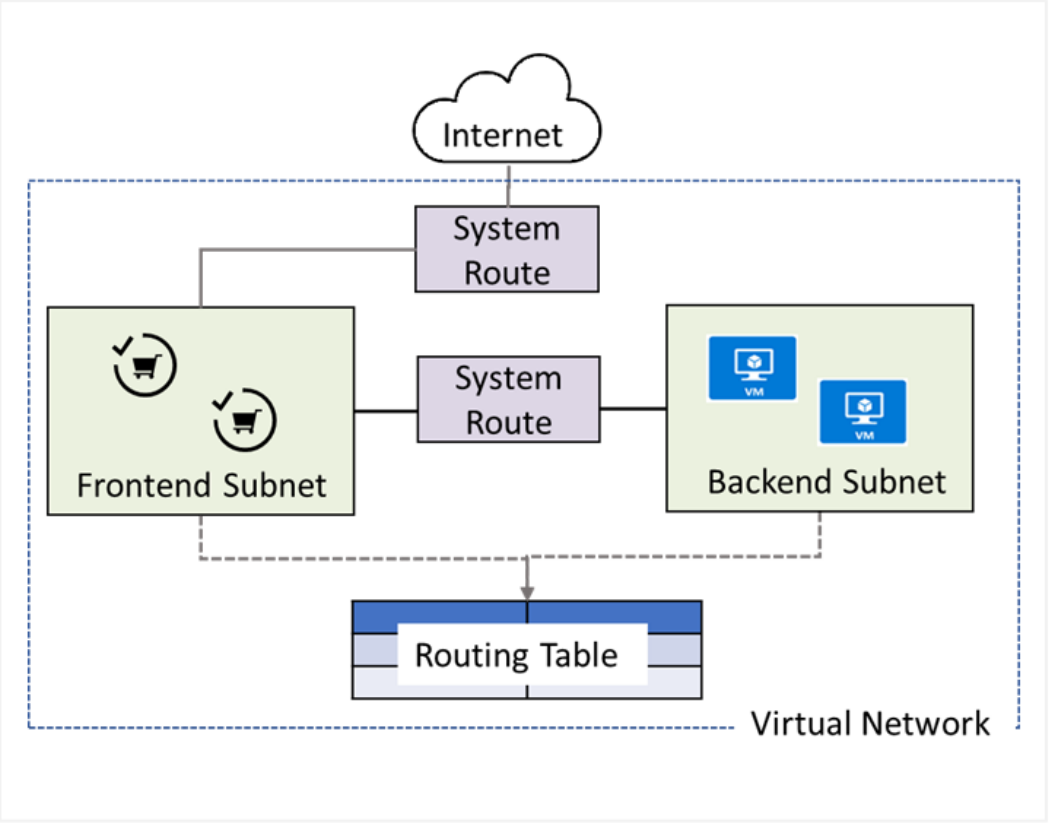
Service Endpoint Services

Private Link

System Routes

System routes direct network traffic between virtual machines, on-premises networks, and the Internet:

- Traffic between VMs in the same subnet
- Between VMs in different subnets in the same virtual network
- Data flow from VMs to the Internet
- Communication between VMs using a VNet-to-VNet VPN
- Site-to-Site and ExpressRoute communication through the VPN gateway

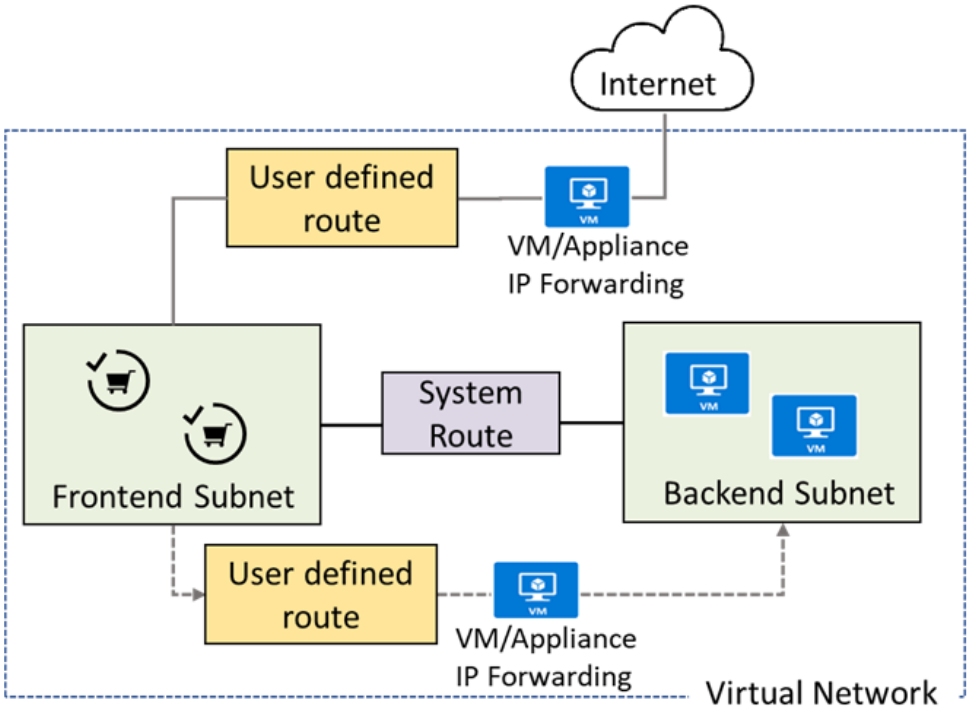


User Defined Routes

A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network

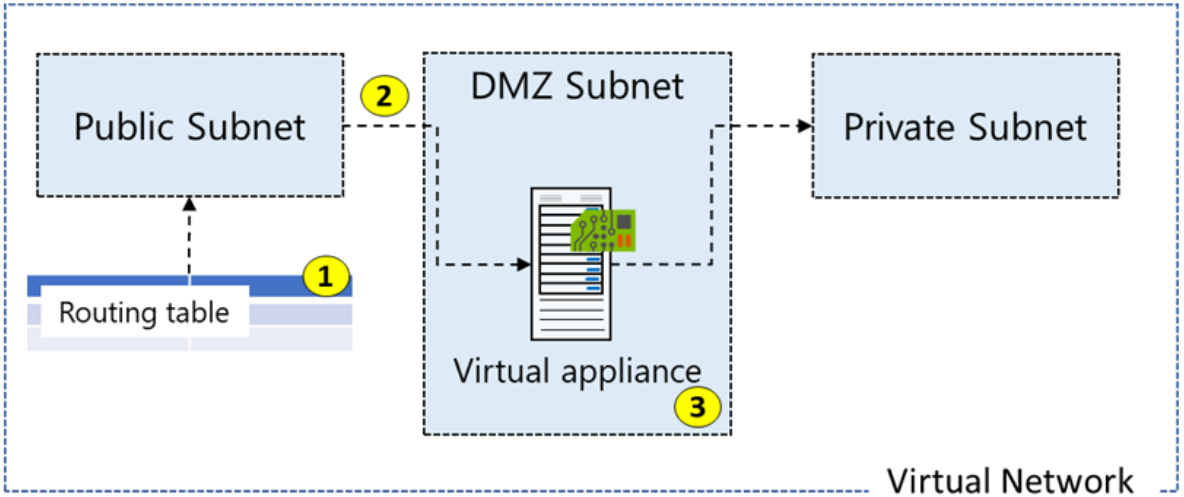
User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow

The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance



Routing Example

All traffic coming into the public subnet and headed for the private subnet must be go through the virtual network appliance



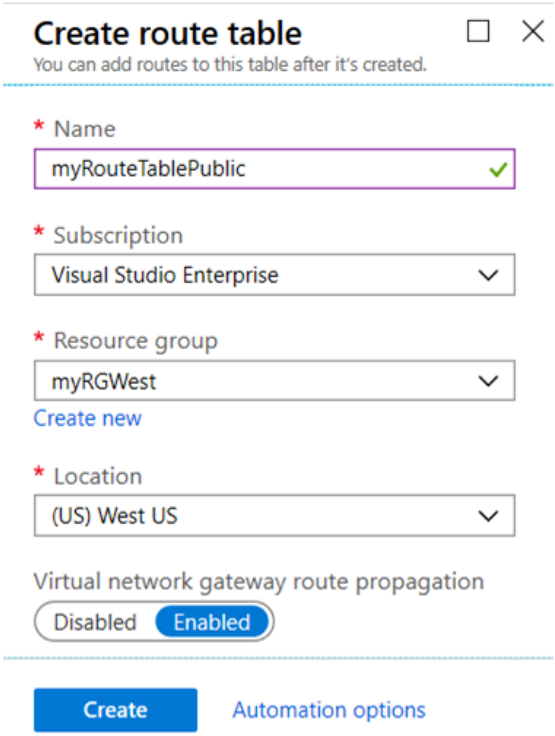
1. Create a routing table
2. Add a custom route that requires all private subnet traffic be directed to a network appliance
3. Associate the new route to the public subnet

Create a Routing Table

A standard routing protocol is used to exchange routing and reachability information between two or more networks

Routes are automatically added to the route table of all subnets with virtual network gateway route propagation enabled

In most situations you will want to enable route propagation

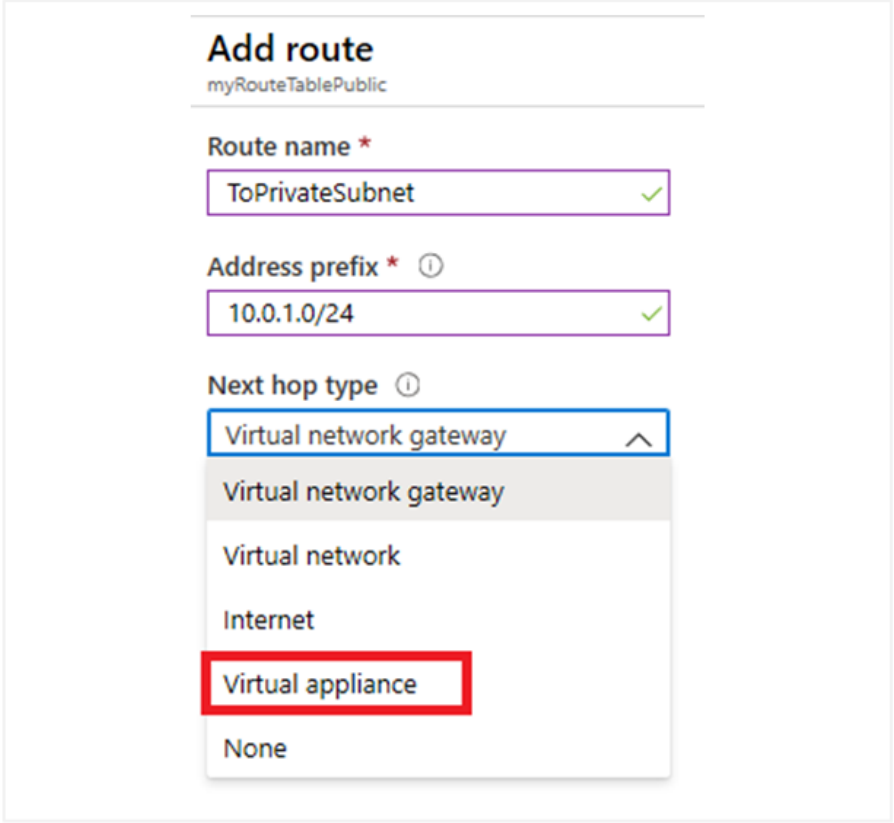


Create a Custom Route

When you create a route there are several Next hop types

In this example, any private subnet IP addresses will be sent to the virtual appliance

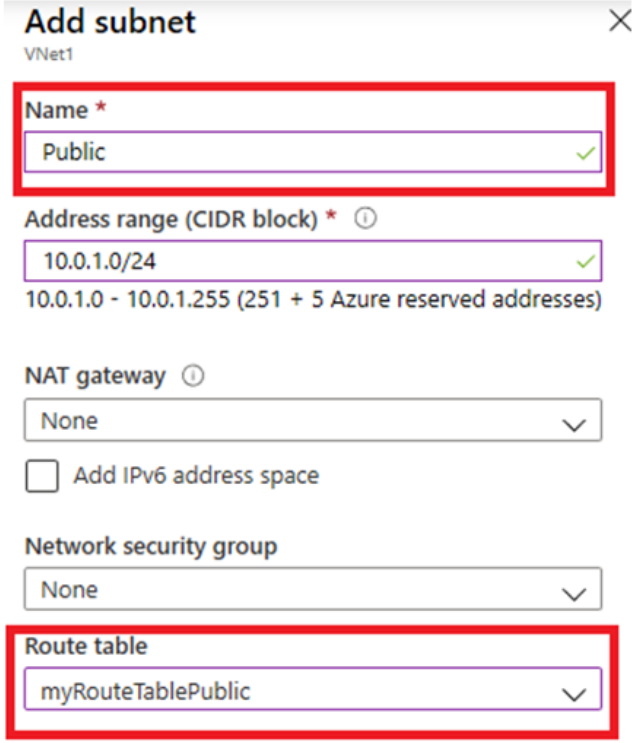
Other choices are Virtual network gateway, Virtual network, Internet, and None



Associate the Route Table

Each subnet can have zero or one route table associated to it

In our example, the Public subnet will be associated with the routing table



Service Endpoints

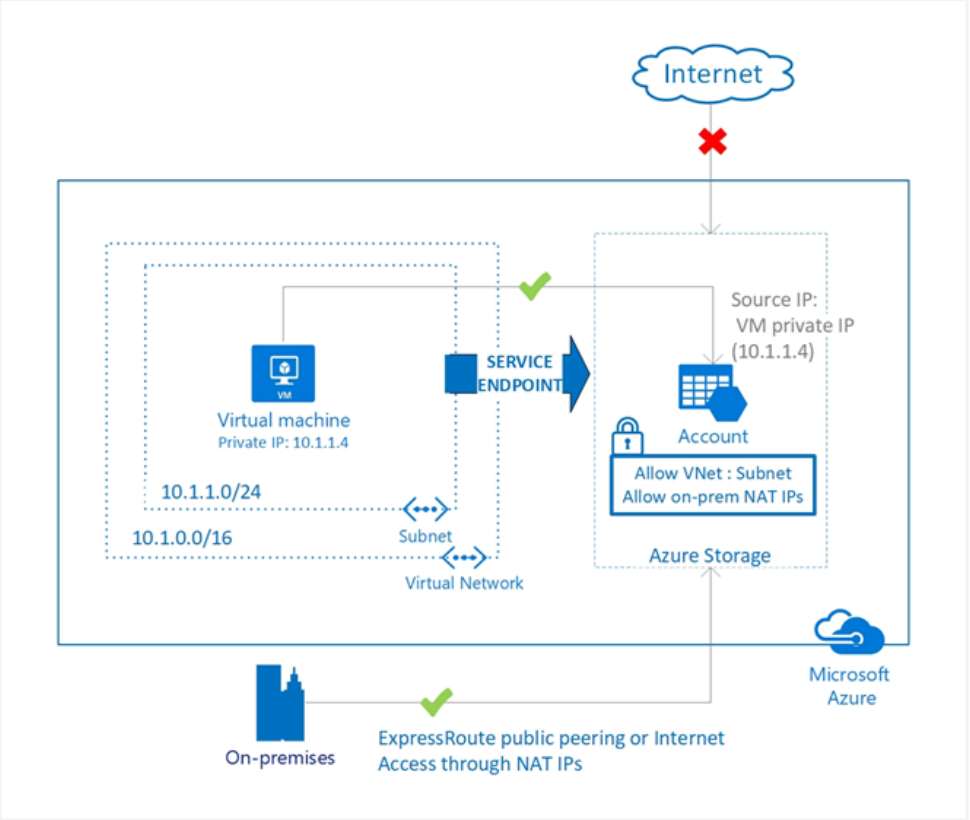
Endpoints limit network access to specific subnets and IP addresses

Improved security for your Azure service resources

Optimal routing for Azure service traffic from your virtual network

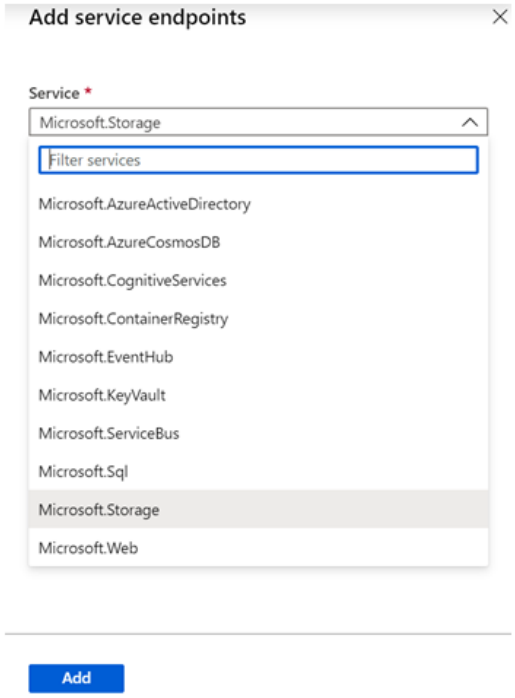
Endpoints use the Microsoft Azure backbone network

Simple to set up with less management overhead



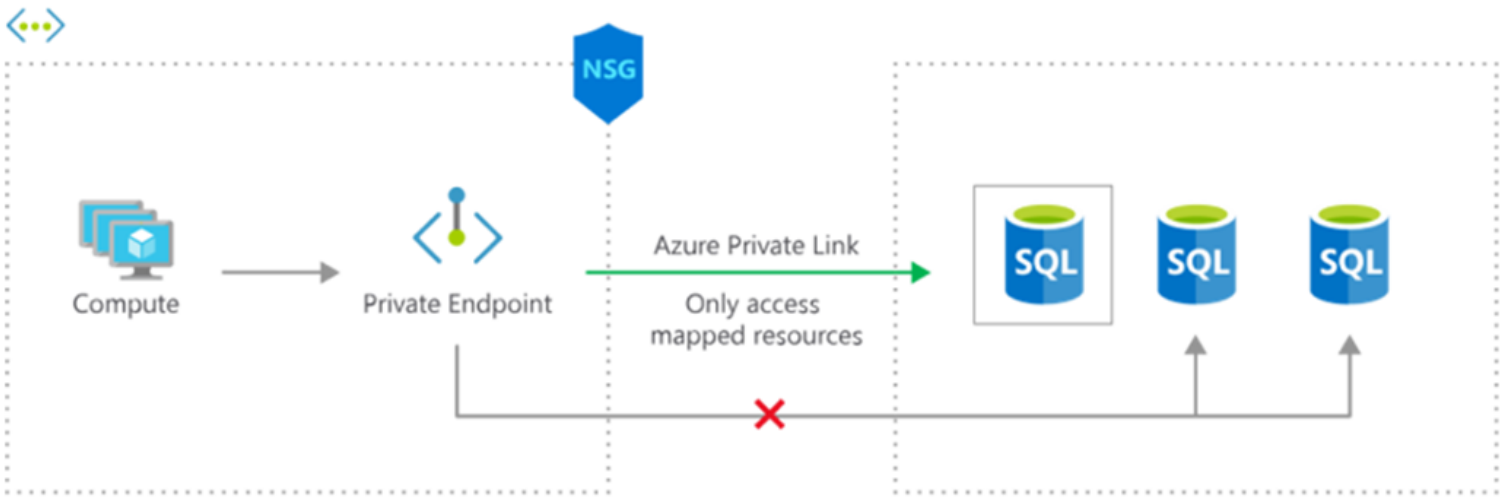
Service Endpoint Services

There are many types of service endpoints



Adding service endpoints can take up to 15 minutes to complete

Private Link



Private connectivity to services on Azure. Traffic remains on the Microsoft network, with no public internet access

Integration with on-premises and peered networks

In the event of a security incident within your network, only the mapped resource would be accessible

Lesson 02: Azure Load Balancer

Azure Load Balancer Overview

Azure Load Balancer

Backend Pools

Public Load Balancer

Load Balancer Rules

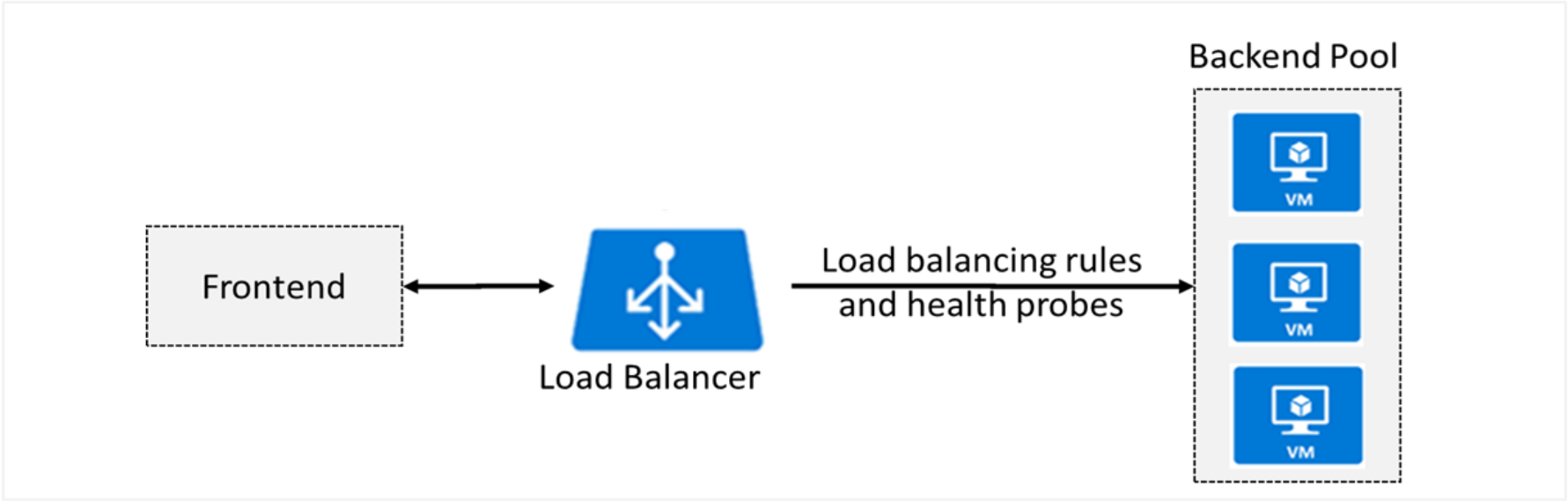
Internal Load Balancer

Session Persistence

Load Balancer SKUs

Health Probes

Azure Load Balancer

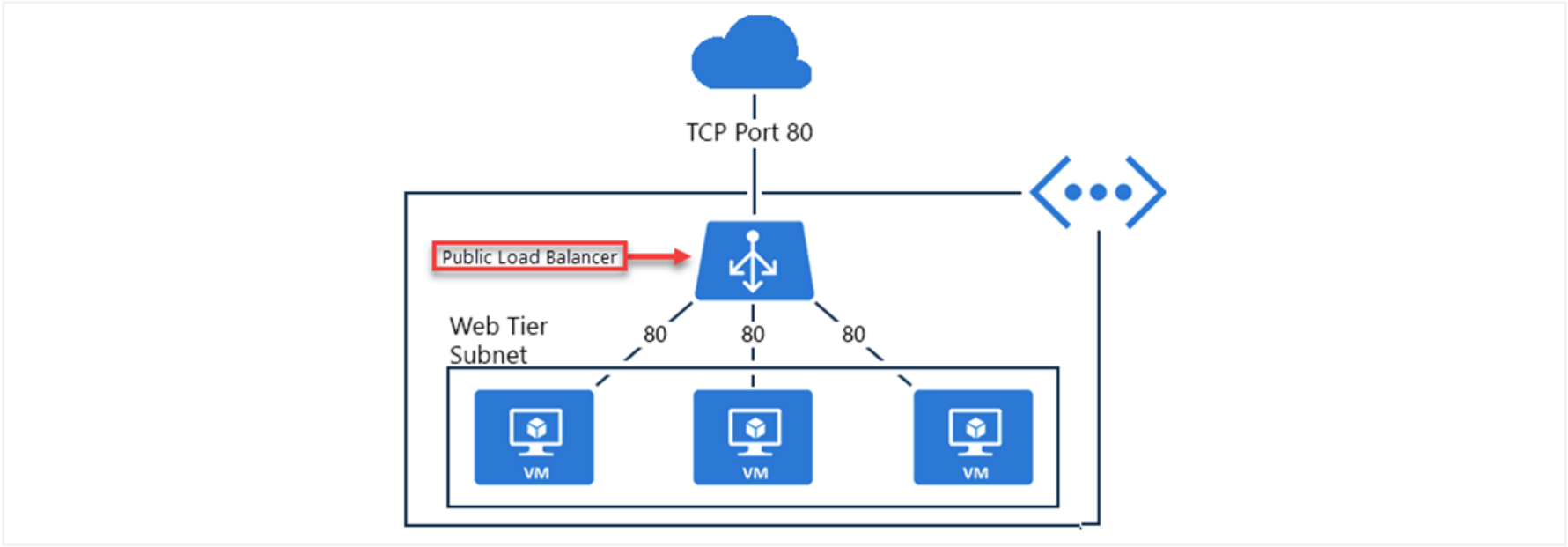


Distributes inbound traffic to backend resources using load-balancing rules and health probes

Can be used for both inbound/outbound scenarios

Two types: Public and Internal

Public Load Balancer



Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number, and vice versa

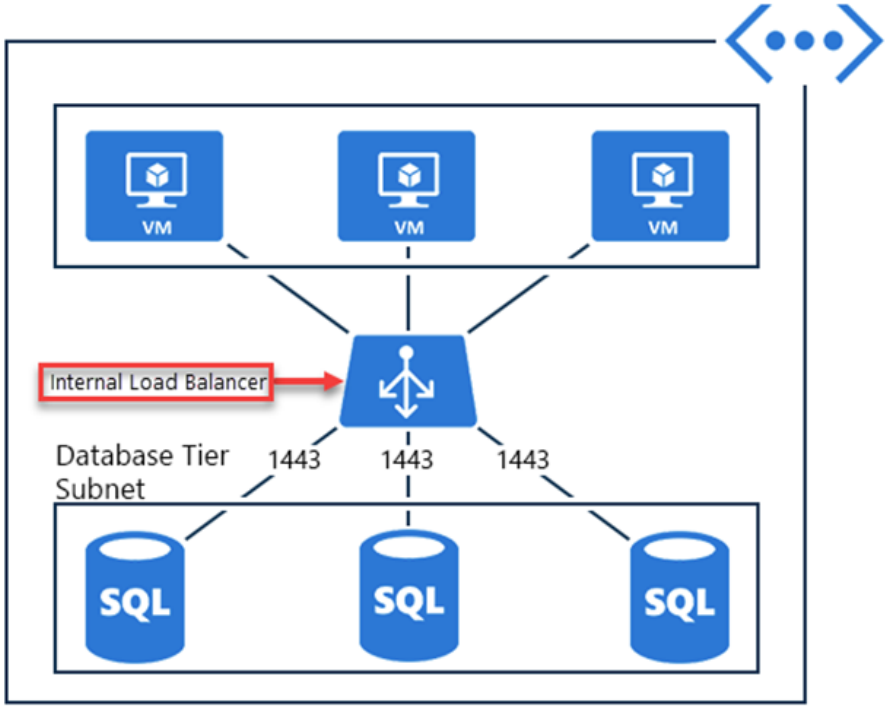
Apply load balancing rules to distribute traffic across VMs or services

Internal Load Balancer

Directs traffic only to resources inside a virtual network or that use a VPN to access Azure infrastructure

Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint

Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications



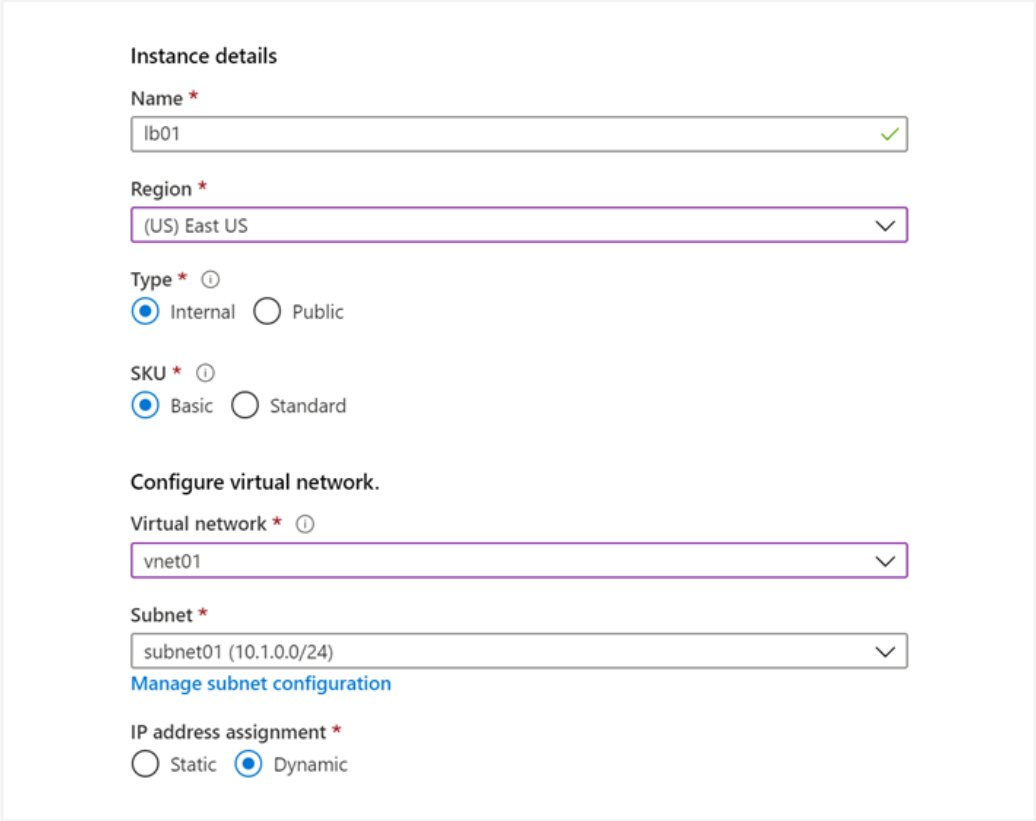
Load Balancer SKUs

Load balancer supports both Basic and Standard (newer) SKUs

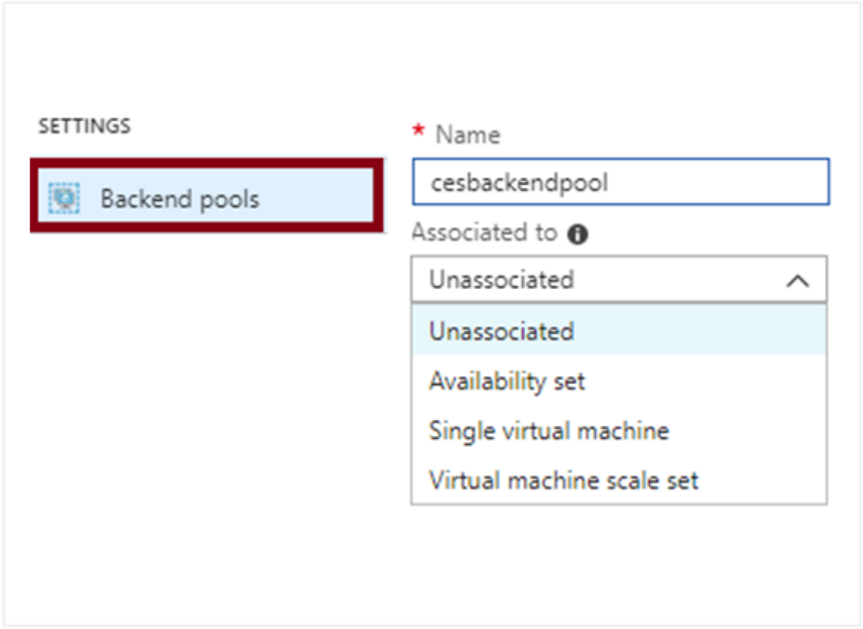
SKUs are not mutable

Only Standard Load Balancer rules can span two virtual networks

No charge for the Basic Load Balancer SKU



Backend Pools



SKU	Backend pool endpoints
Basic SKU	VMs in a single availability set or VM scale set
Standard SKU	Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets

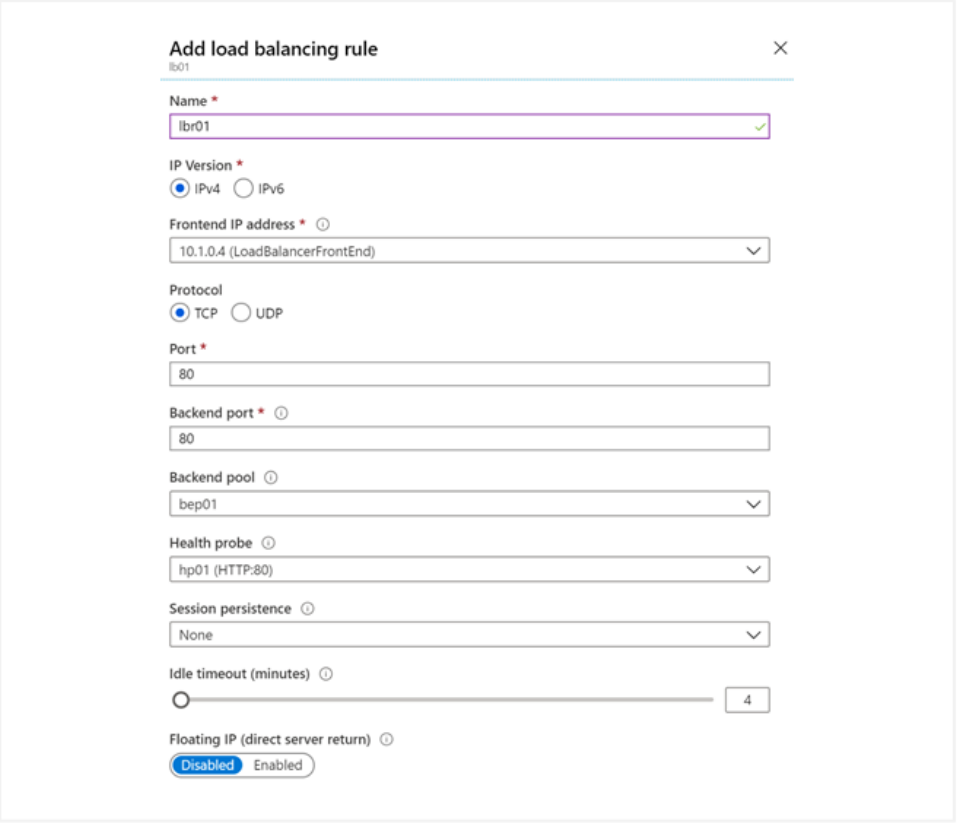
To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer

Load Balancer Rules

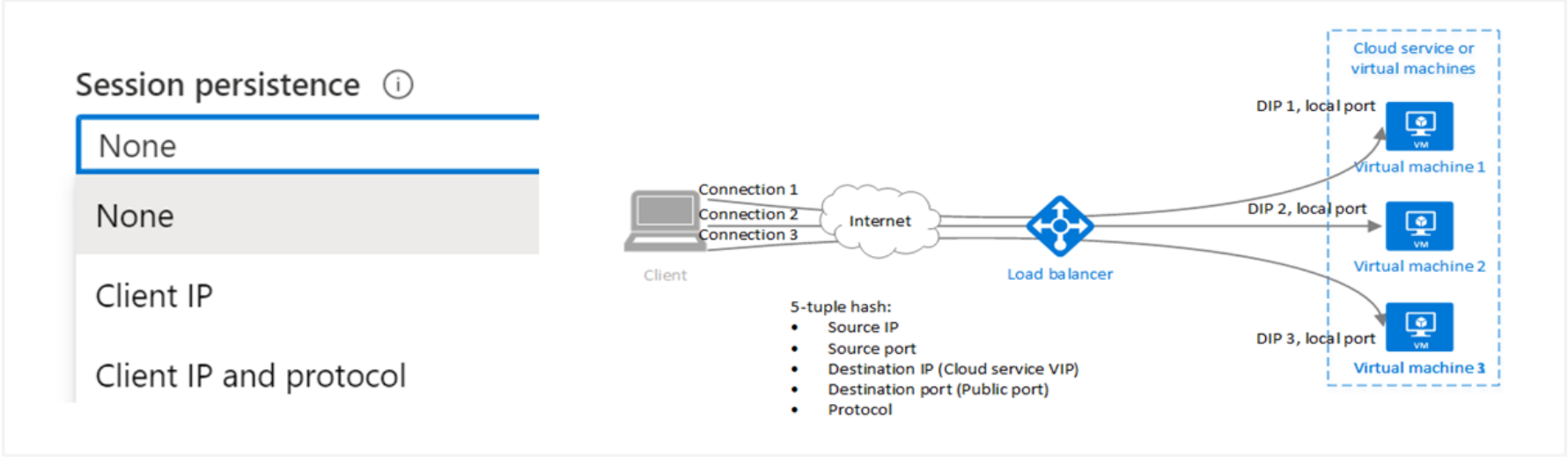
Maps a frontend IP and port combination to a set of backend IP addresses and port combination

Rules can be used in combination with NAT rules

A NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target



Session Persistence



Session persistence specifies how client traffic is handled

None (default) requests can be handled by any virtual machine

Client IP requests will be handled by the same virtual machine

Client IP and protocol specifies that successive requests from the same address and protocol will be handled by the same virtual machine

Health Probes

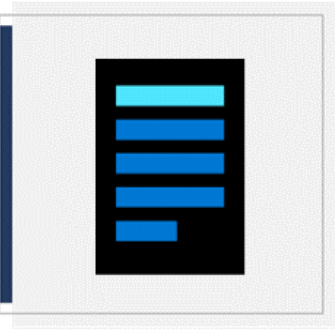
Allows the load balancer to monitor the status of an app

Dynamically adds or removes VMs from the load balancer rotation based on their response to health checks

HTTP custom probe (preferred) pings every 15 seconds

TCP custom probe tries to establish a successful TCP session

Lesson 03: Azure Application Gateway



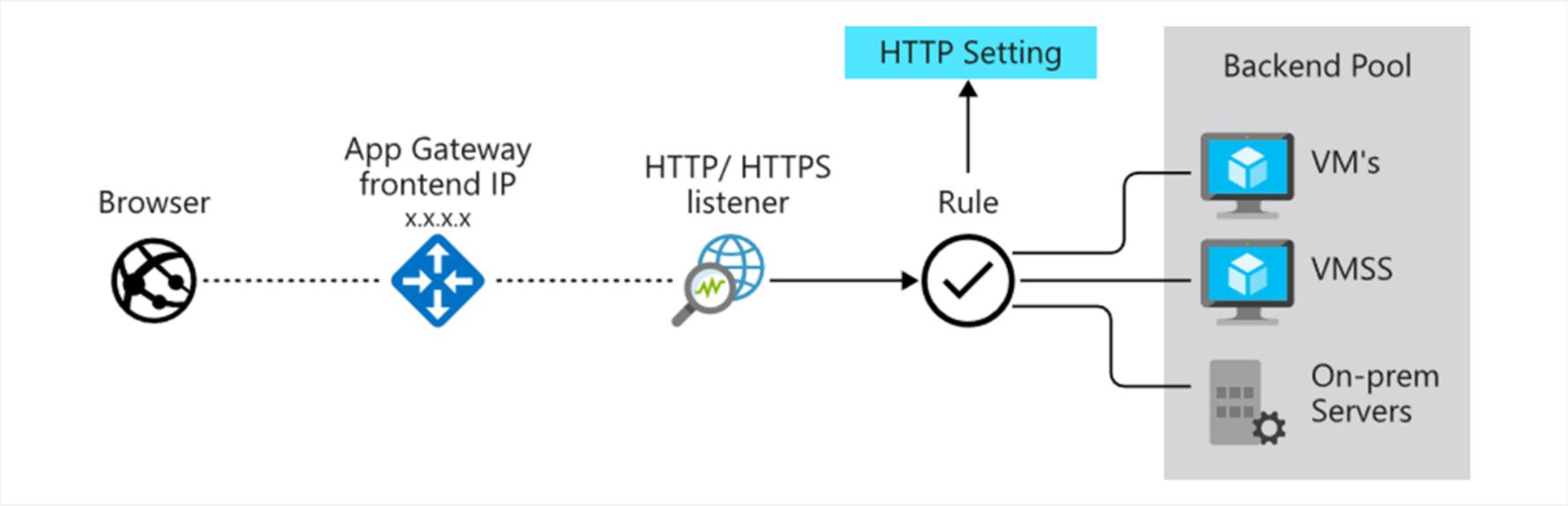
Application Gateway Overview

Application Gateway

Application Gateway Routing

Application Gateway Configuration

Application Gateway



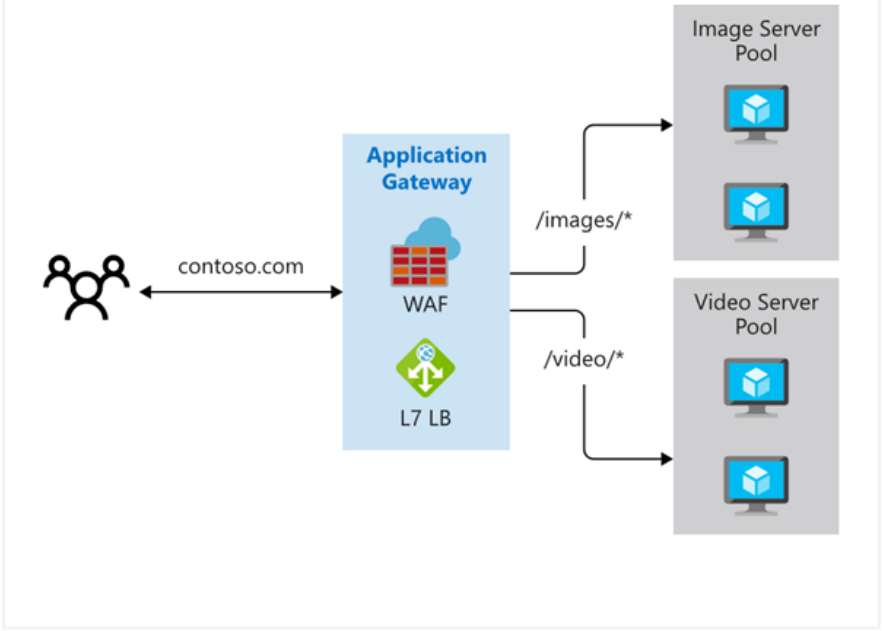
Manages web app requests

Routes traffic to a pool of web servers based on the URL of a request

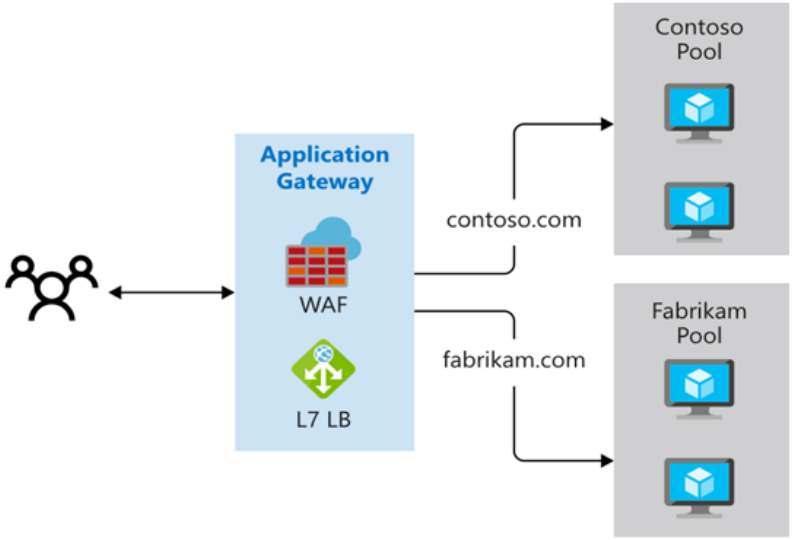
The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Application Gateway Routing

Path-based routing

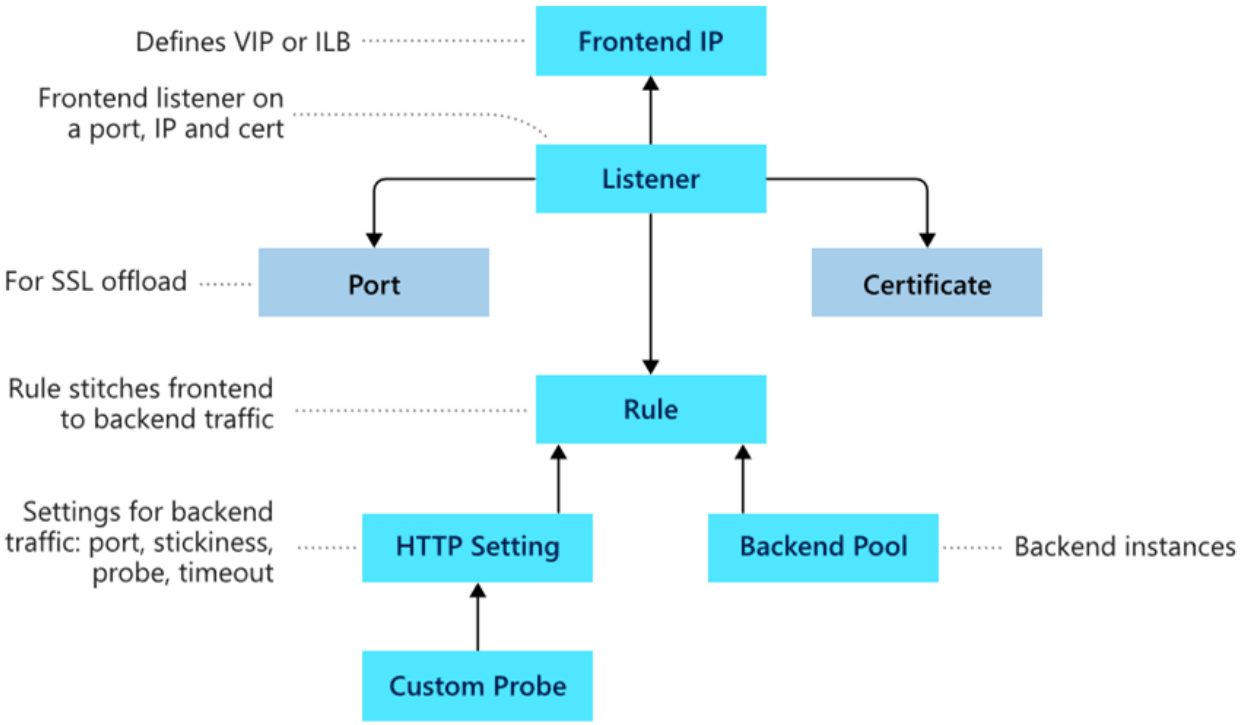


Multiple-site routing



Application Gateway Components

- Frontend IP
- Listeners
- Routing rules
- Backend pools
- Web application firewall (optional)
- Health probes



Microsoft Azure

Module 07: Azure Storage

Module Overview

Lesson 01: Storage Accounts

Lesson 02: Blob Storage

Lesson 03: Storage Security

Lesson 04: Azure Files and File Sync

Lesson 05: Managing Storage

Lesson 01: Storage Accounts

Storage accounts overview

Azure Storage

Azure Storage Services

Storage Account Kinds

Replication Strategies

Accessing Storage

Securing Storage Endpoints

Azure Storage

A service that you can use to store files, messages, tables, and other types of information

Durable, secure, scalable, managed, accessible

Storage for virtual machines, unstructured data and structured data

Two tiers: Standard (HDD magnetic drives) and Premium (SSD)

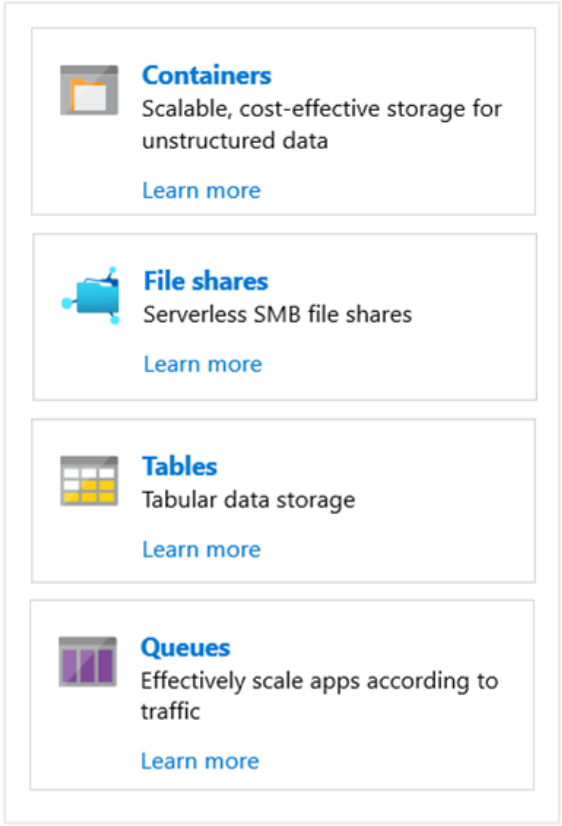
Azure Storage Services

Azure Containers: A massively scalable object store for text and binary data

Azure Files: Managed file shares for cloud or on-premises deployments

Azure Tables: A NoSQL store for schemaless storage of structured data

Azure Queues: A messaging store for reliable messaging between application components



Storage Account Kinds

Storage account type	Supported services	Supported tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
Storage (general purpose v1)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
StorageV2 (general purpose v2)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
File Storage	Files only	Premium	LRS, ZRS (limited regions)

All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest

Replication Strategies

Data Replication Options	Description
Locally redundant storage (LRS)	Data is replicated three times within a single facility in a single region
Zone-redundant storage (ZRS)	Data is replicated across multiple Availability Zones within one region
Geo-redundant storage (GRS)	Data is replicated three times within the primary region and replicated three times to the regions pair.
Read access geo-redundant storage (RA-GRS)	Data is replicated three times within the primary region and replicated with read-access to the region pair
Geo-zone-redundant storage (GZRS)	Data is replicated across three Availability Zones and replicated to the region pair
Read-access Geo-zone-redundant storage (RA-GZRS)	Data is replicated across three Availability Zones and replicated with read-access to the region pair

Accessing Storage

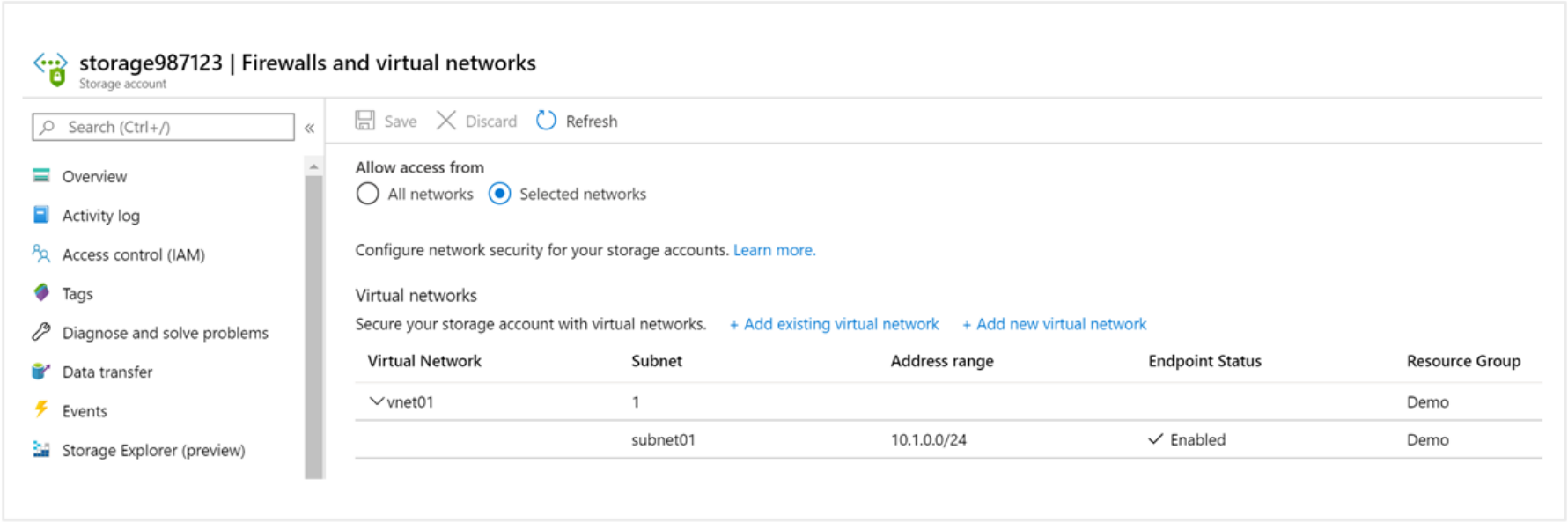
Every object has a unique URL address – based on account name and storage type

CNAME record	Target
blobs.contoso.com	contosoblobs.blob.core.windows.net

Container service: http://*mystorageaccount*.blob.core.windows.net
Table service: http://*mystorageaccount*.table.core.windows.net
Queue service: http://*mystorageaccount*.queue.core.windows.net
File service: http://*mystorageaccount*.file.core.windows.net

If you prefer you can configure a custom domain name

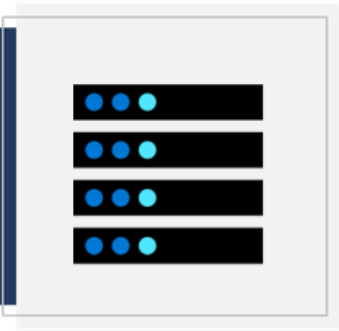
Securing Storage Account Endpoints



Firewalls and Virtual Networks allows for restricting access to the Storage Account from specific Subnets on Virtual Networks

Subnets and Virtual Networks must exist in the same Azure Region or Region Pair as the Storage Account

Lesson 02: Blob Storage



Blob Storage Overview

Blob Storage

Blob Containers

Blob Access Tiers

Blob Lifecycle Management

Uploading Blobs

Storage Pricing

Blob Storage

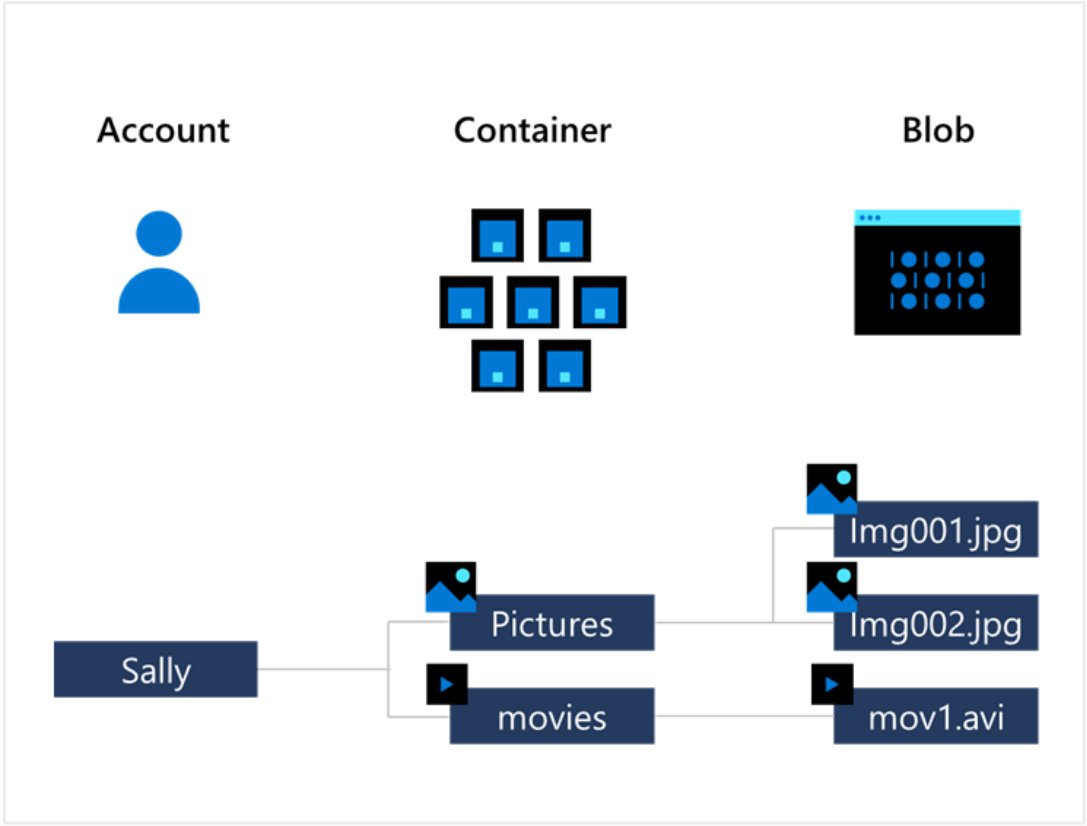
Stores unstructured data in the cloud

Can store any type of text or binary data

Also referred to as *object storage*

Common uses:

- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Storing data for backup and restore, disaster recovery, archiving
- Storing data for analysis by an on-premises or Azure-hosted service



Blob Containers

All blobs must be in a container

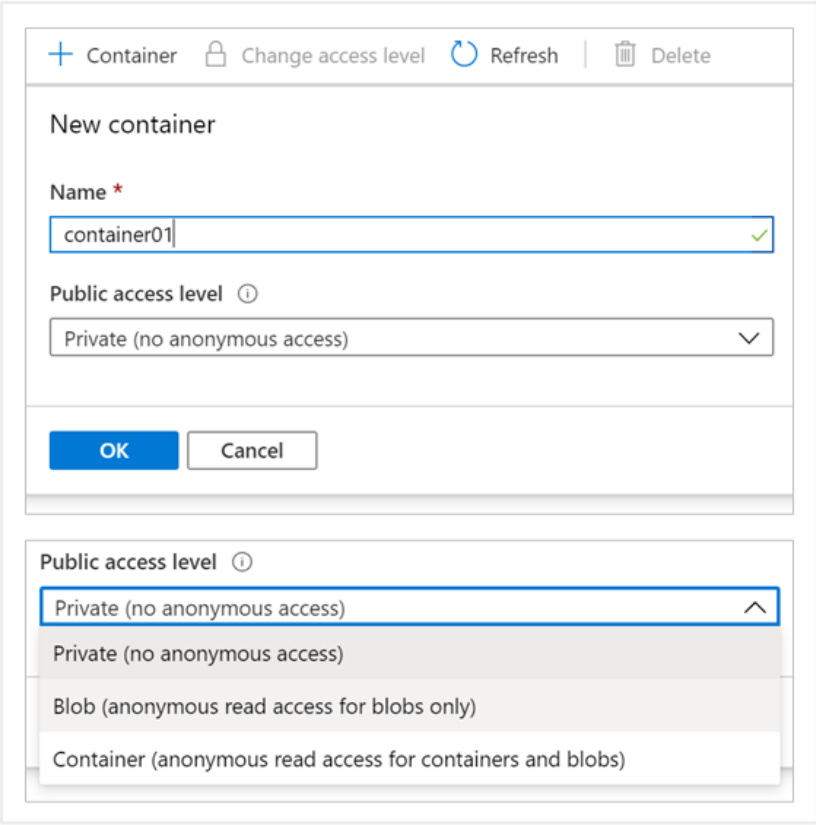
Accounts have unlimited containers

Containers can have unlimited blobs

Private blobs – no anonymous access

Blob access – anonymous public read access for blobs only

Container access – anonymous public read and list access to the entire container, including the blobs

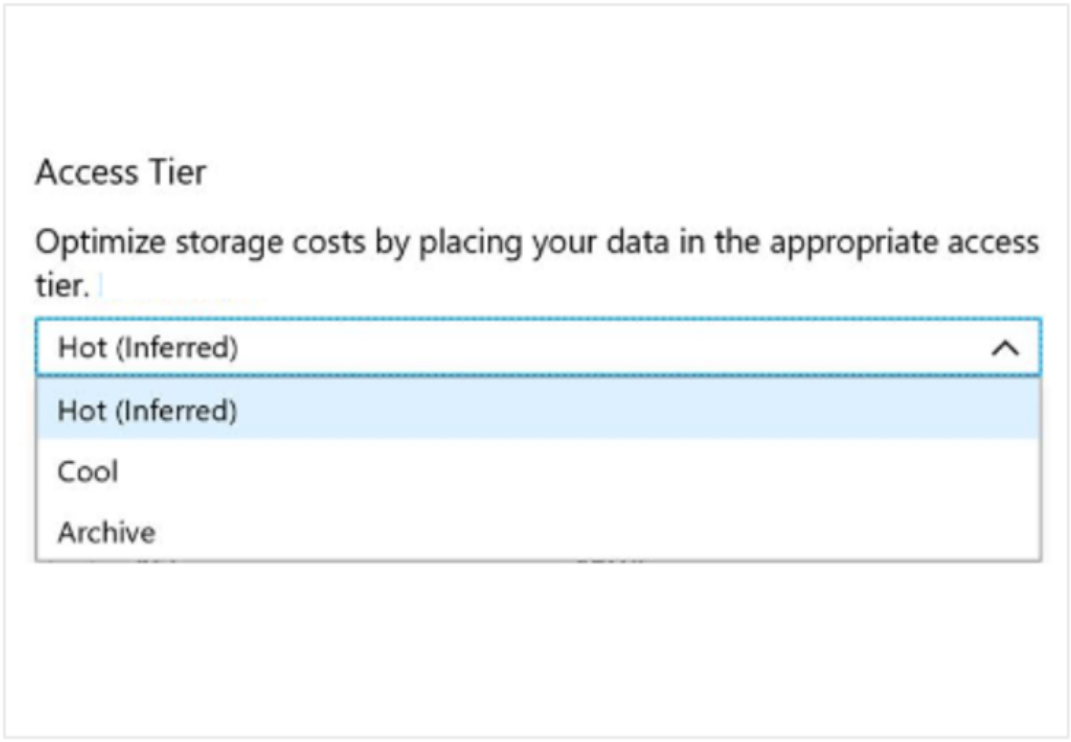


Blob Access Tiers

Hot tier – Optimized for frequent access of objects in the storage account

Cool tier – Optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days

Archive – Optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days



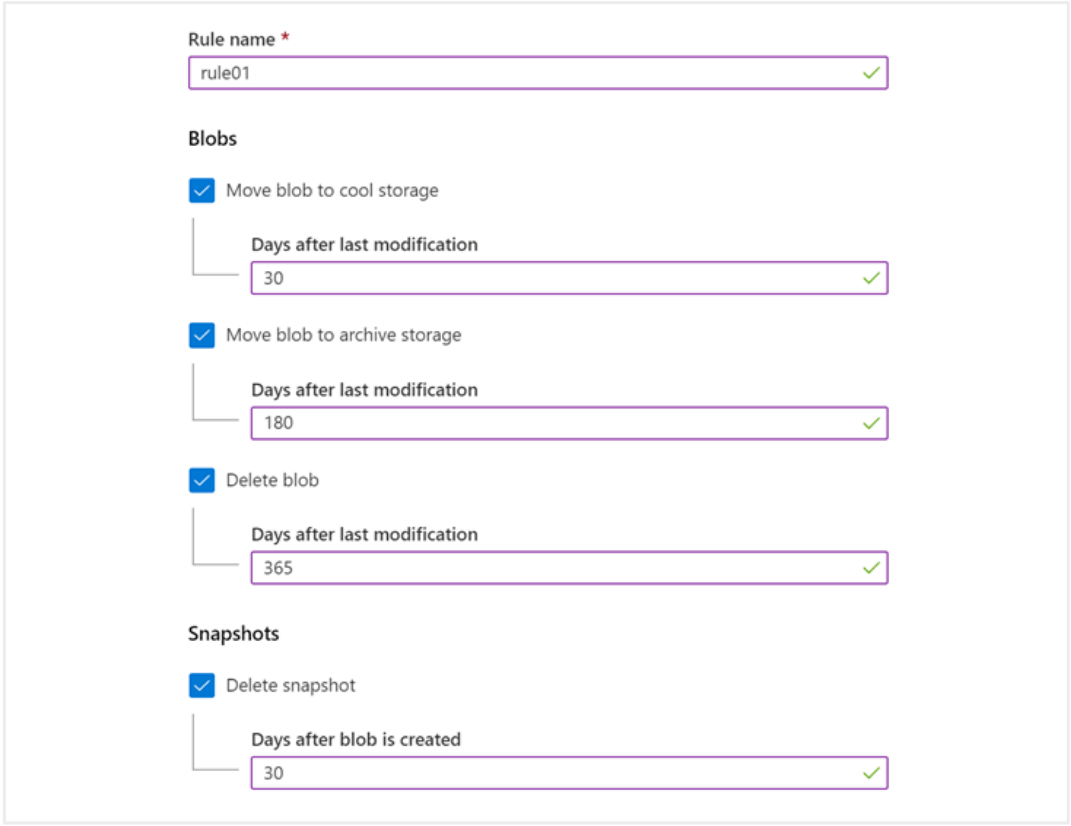
✓ **You can switch between these access tiers at any time**

Blob Lifecycle Management

Transitioning of blobs to a cooler storage tier to optimize for performance and cost

Delete blobs at the end of their lifecycle

Apply rules to filtered paths in the Storage Account



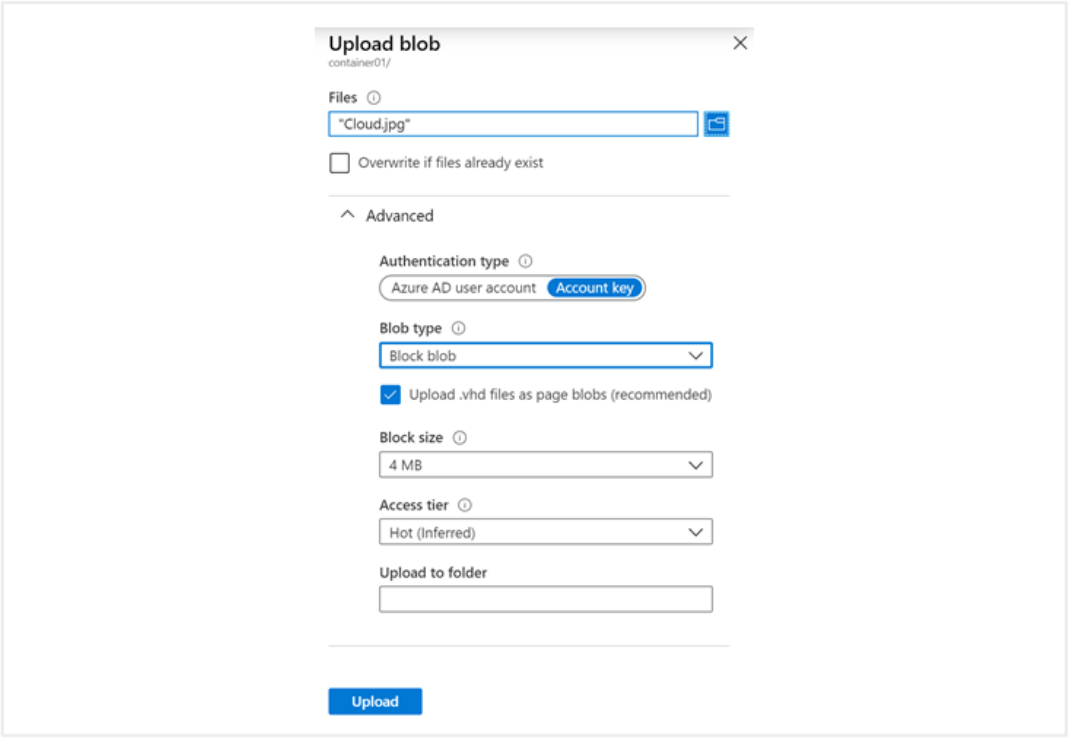
Uploading Blobs

Block blobs (default) – useful for storing text or binary files

Page blobs – more efficient for frequent read/write operations

Append blobs – useful for logging scenarios

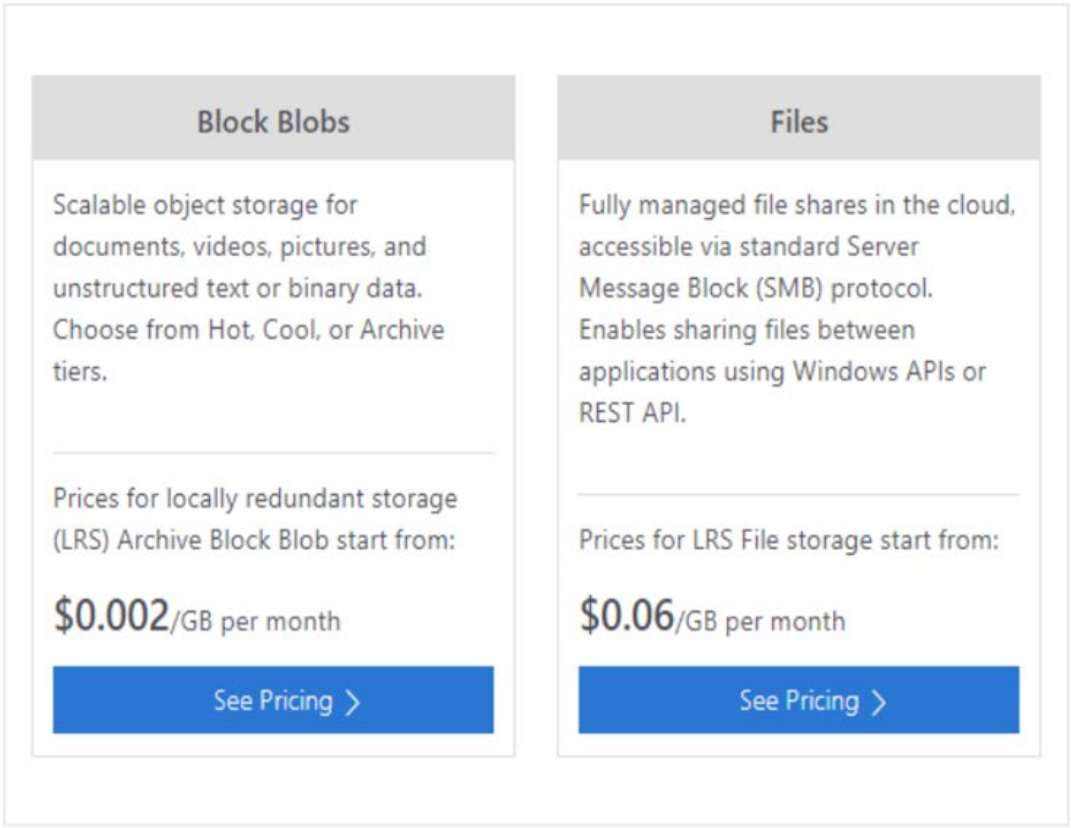
Access tier – select either Hot, Cool, or Archive



✓ You cannot change a blob type once it has been created

Storage Pricing

- Storage costs
- Blob storage
- Data access costs
- Transaction costs
- Geo-Replication data transfer costs
- Outbound data transfer costs
- Changing the storage tier



Lesson 03: Storage Security

Storage Security Overview

Storage Security

Storage Service Encryption

Shared Access Signatures

Customer Managed Keys

URI and SAS Parameters

Storage Security Best Practices

Storage Security

Storage Encryption Services

Authentication with Azure AD and RBAC

Client-side encryption, HTTPS, and SMB 3.0 for data in transit

Azure disk encryption

Shared Access Signatures – delegated access

Shared Key – encrypted signature string

Anonymous access to containers and blobs

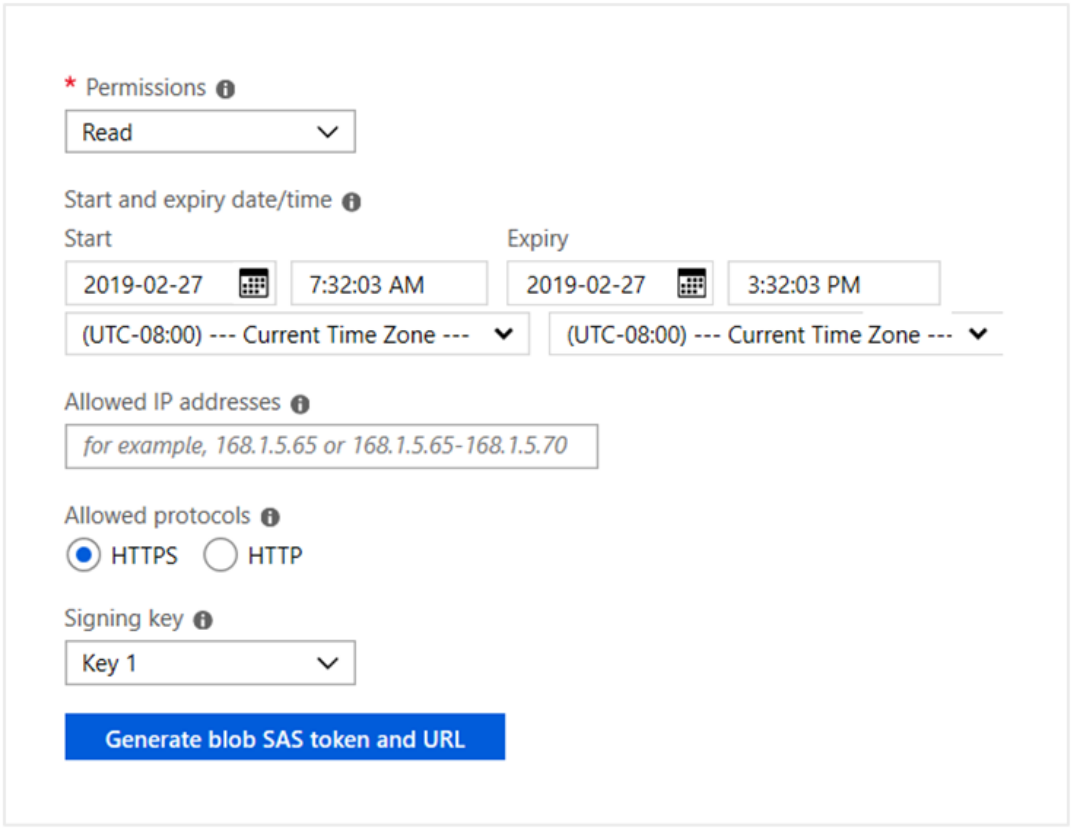
Shared Access Signatures

Provides delegated access to resources

Grants access to clients without sharing your storage account keys

The account SAS delegates access to resources in one or more of the storage services

The service SAS delegates access to a resource in just one of the storage services



URI and SAS Parameters

- A SAS is a signed URI that points to one or more storage resources
- Consists of a storage resource URI and the SAS token


```
https://myaccount.blob.core.windows.net/?sp=r&st=2020-05-
11T18:31:43Z&se=2020-05-12T02:31:43Z&spr=https&sv=2019-10-
10&sr=b&sig=jOqABJZHfUVeBQ3yVn7kWiCKlO0sxCiK1rzEchfAz8U%3D
```

Includes parameters for resource URI, storage services version, services, resource types, start time, expiry time, resource, permissions, IP range, protocol, signature

Storage Service Encryption

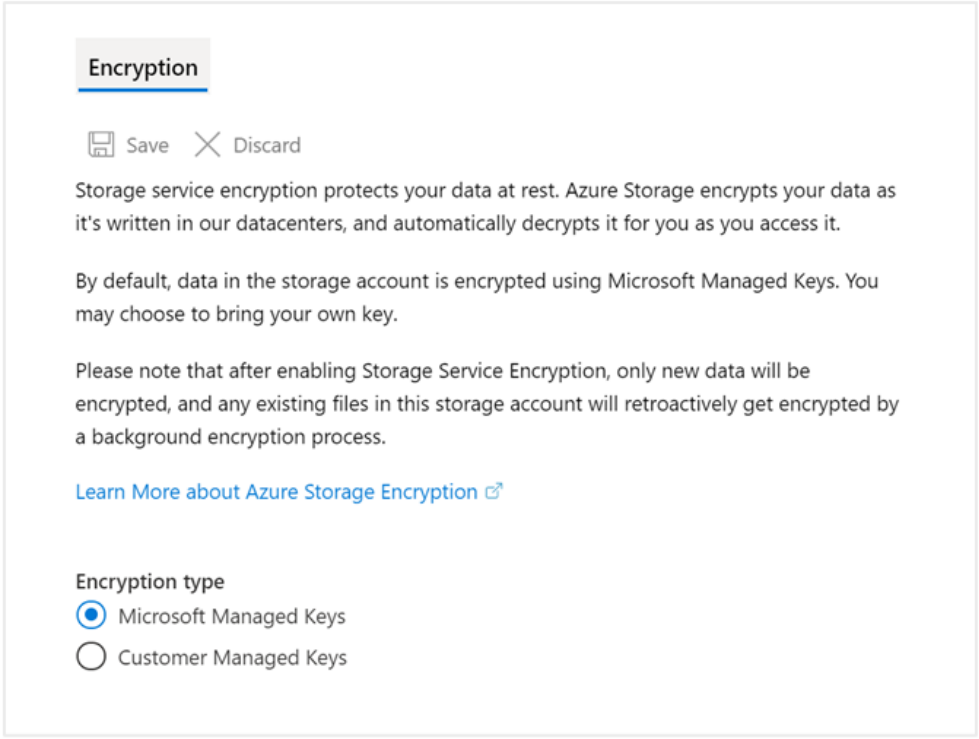
Protects your data for security and compliance

Automatically encrypts and decrypts your data

Encrypted through 256-bit AES encryption

Is enabled for all new and existing storage accounts and cannot be disabled

Is transparent to users



You can use your own key (next topic)

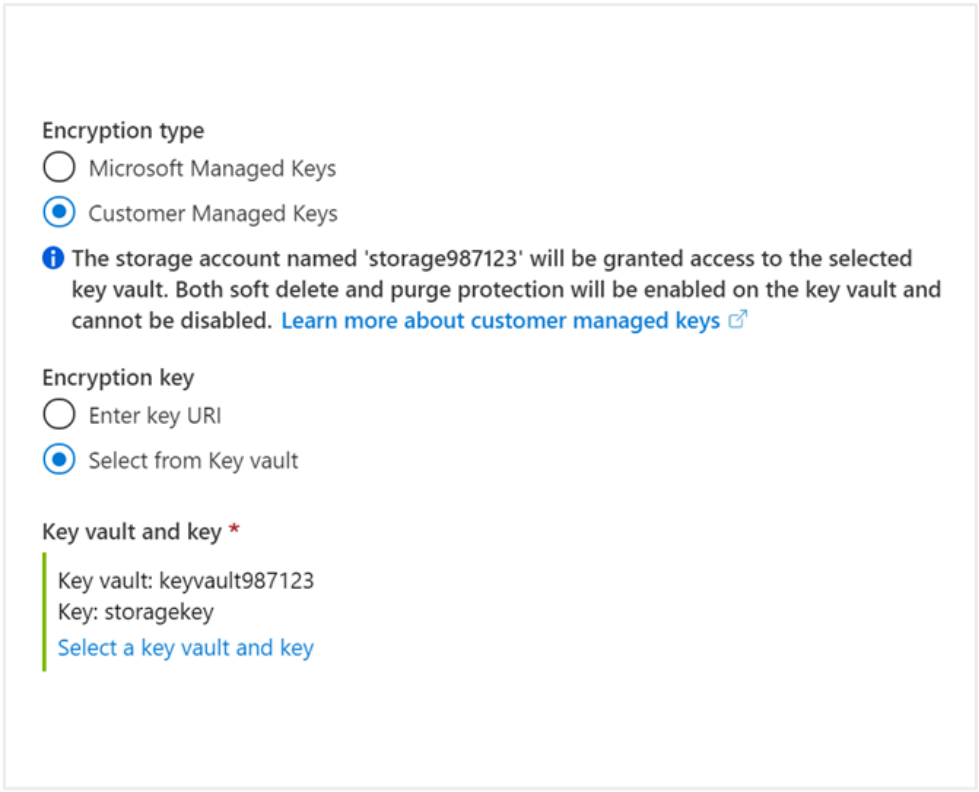
Customer Managed Keys

Use the Azure Key Vault to manage your encryption keys

Create your own encryption keys and store them in a key vault

Use Azure Key Vault's APIs to generate encryption keys

Custom keys give you more flexibility and control



Storage Best Practices

Always use HTTPS to create or distribute an SAS

Reference stored access policies where possible

Use near-term expiration times on an ad hoc SAS

Have clients automatically renew the SAS if necessary

Be careful with SAS start time

Be specific with the resource to be accessed

Understand that your account will be billed for any usage

Validate data written using SAS

Don't assume SAS is always the correct choice

Use Storage Analytics to monitor your application

Lesson 04: Azure Files and File Sync

Azure Files and File Sync Overview

Files vs Blobs

Azure File Sync

Managing File Shares

Azure File Sync Components

File Share Snapshots

File Sync Steps

Files vs Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files	• Lift and shift an application to the cloud • Store shared data across multiple virtual machines • Store development and debugging tools that need to be accessed from many virtual machines
Azure Blobs	Client libraries and a REST interface that allows unstructured data (flat namespace) to be stored and accessed at a massive scale in block blobs	• Support streaming and random-access scenarios • Access application data from anywhere

Managing File Shares

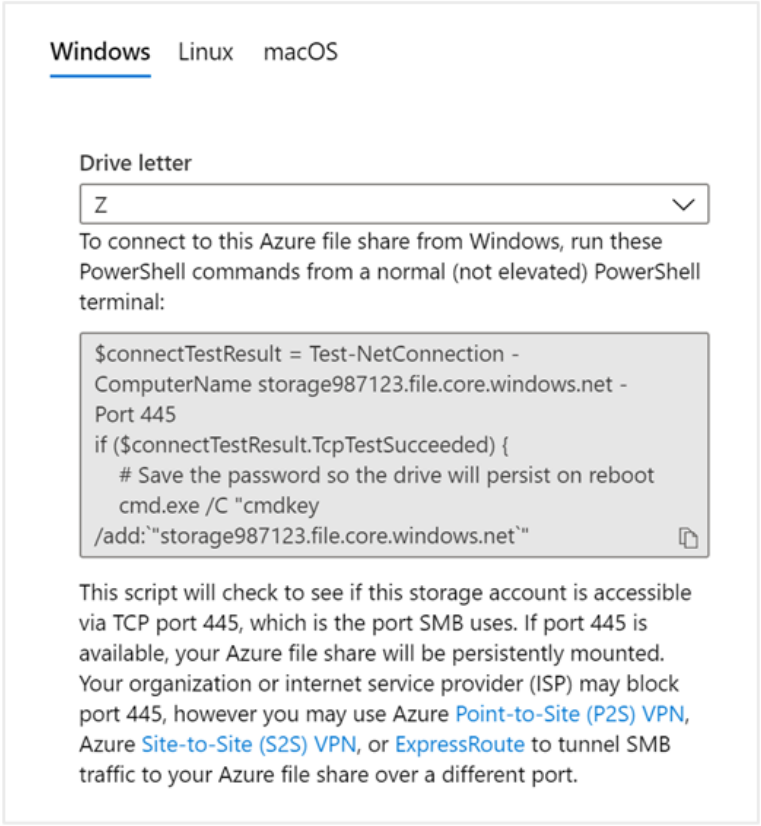
File share quotas

Windows – ensure port 445 is open

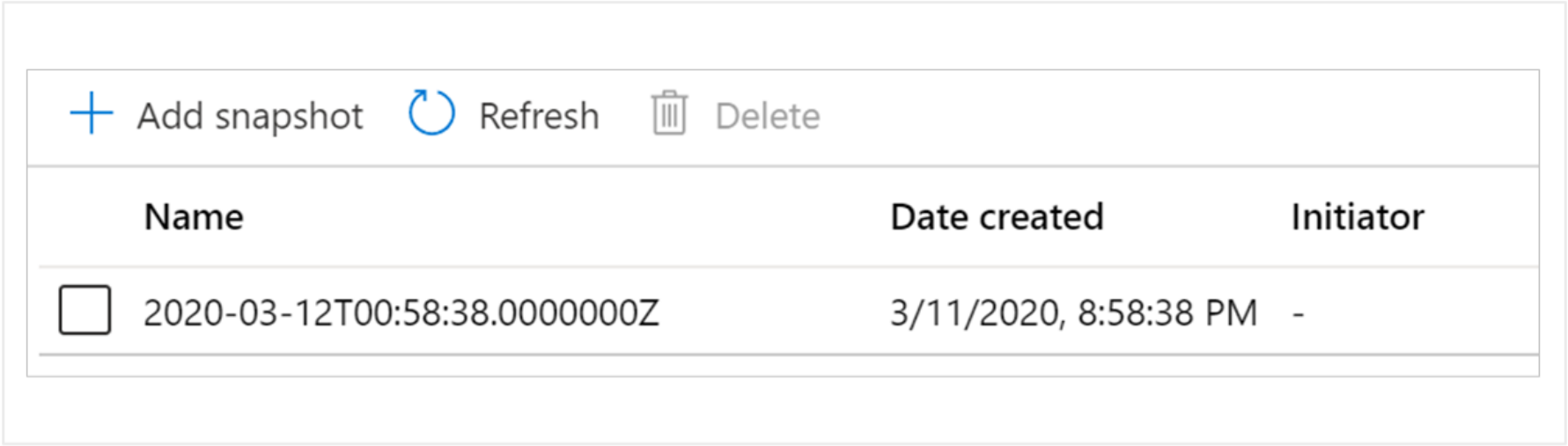
Linux – mount the drive

MacOS – mount the drive

Secure transfer required – SMB 3.0 encryption



File Share Snapshots



Incremental snapshot that captures the share state at a point in time

Is read-only copy of your data

Snapshot at the file share level, and restore at the file level

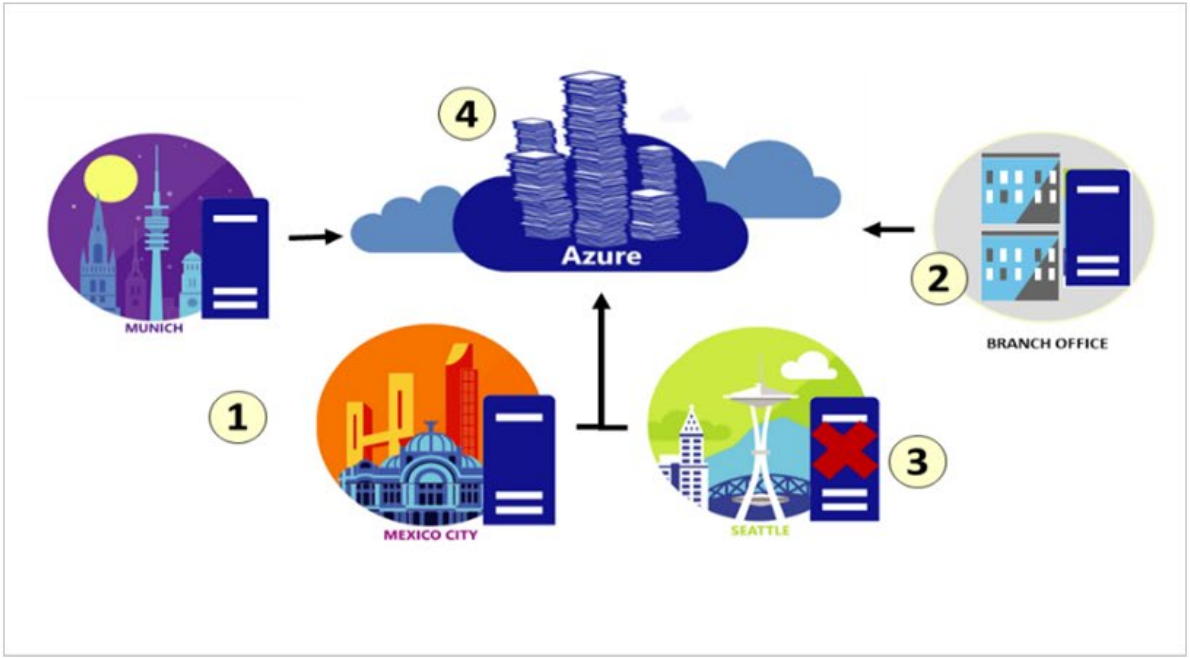
Uses:

- Protection against application error and data corruption
- Protection against accidental deletions or unintended changes
- General backup purposes

Azure File Sync

Centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server

1. Lift and shift
2. Branch Office backups
3. Backup and Disaster Recovery
4. File Archiving



File Sync Components

The **Storage Sync Service** is the top-level resource

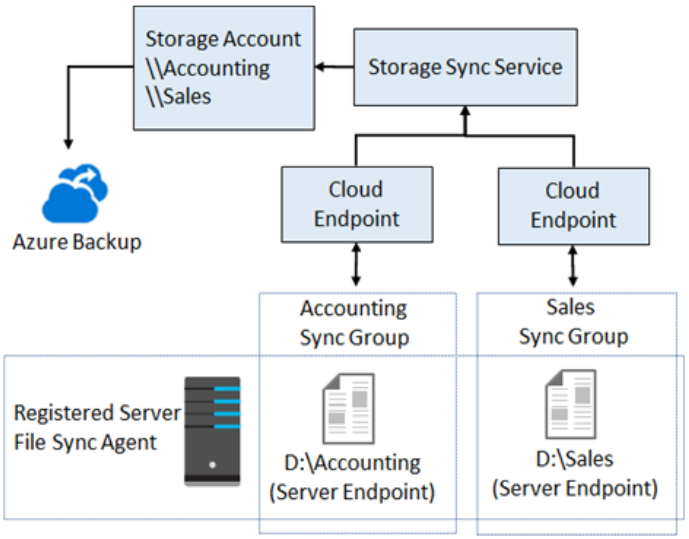
The **registered server** object represents a trust relationship between your server (or cluster) and the Storage Sync Service

The **Azure File Sync agent** is a downloadable package that enables Windows Server to be synced with an Azure file share

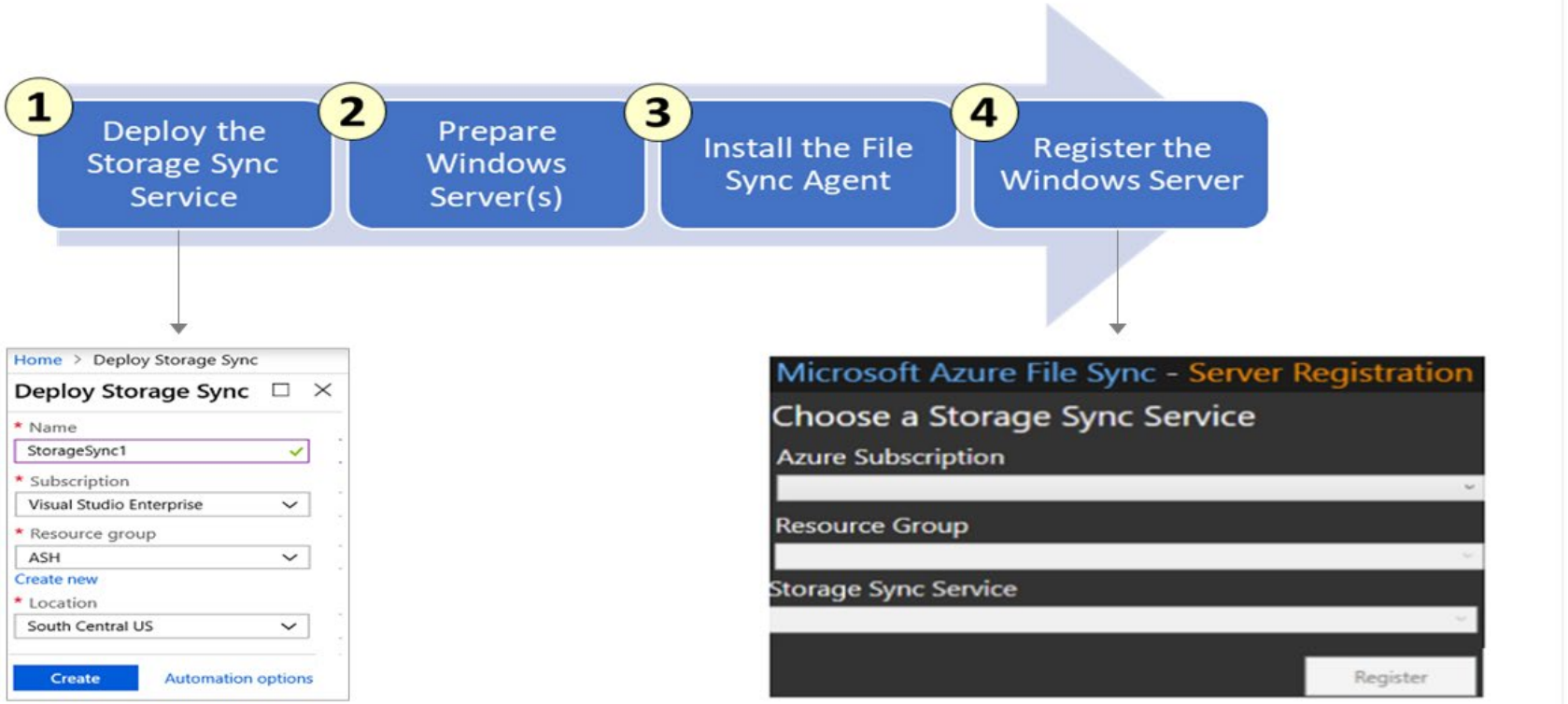
A **server endpoint** represents a specific location on a registered server, such as a folder

A **cloud endpoint** is an Azure file share

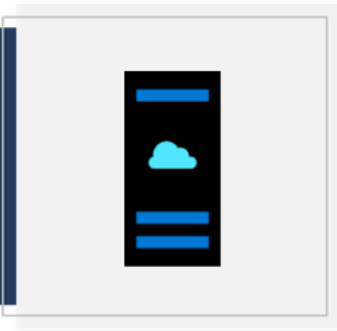
A **sync group** defines which files are kept in sync



File Sync Steps



Lesson 05: Managing Storage



Managing Storage Overview

Storage Explorer

Import and Export Service

AzCopy

Demonstration – Storage Explorer

Storage Explorer

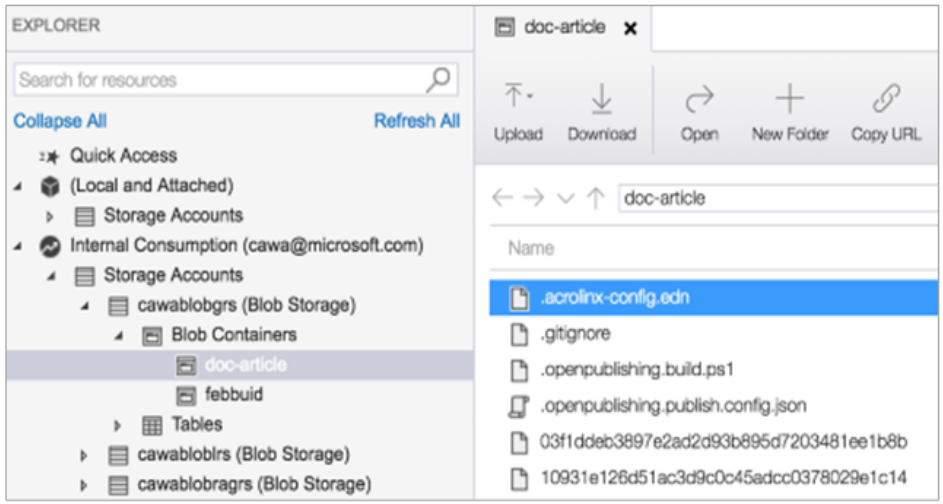
Access multiple accounts and subscriptions

Create, delete, view, edit storage resources

View and edit Blob, Queue, Table, File, Cosmos DB storage and Data Lake Storage

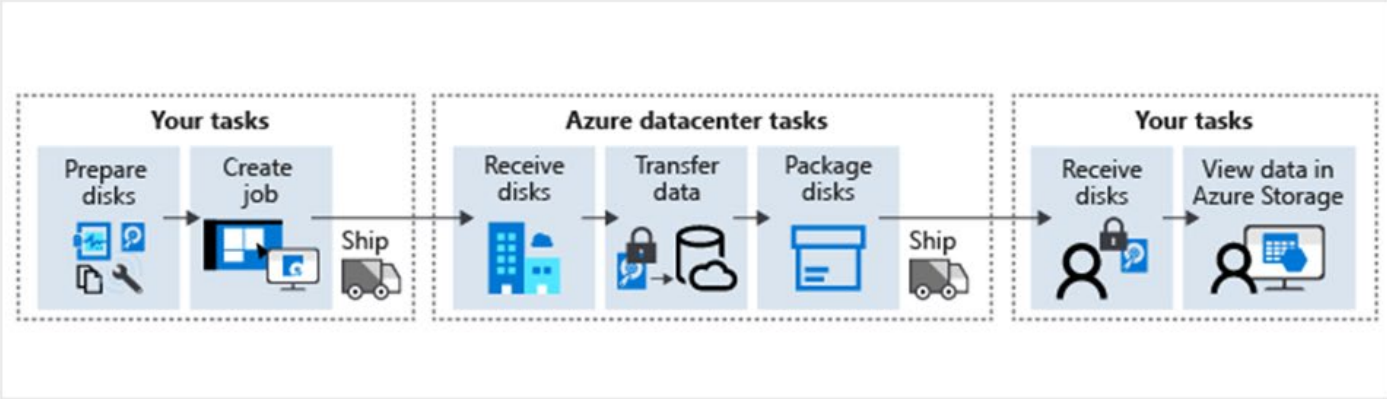
Obtain shared access signature (SAS) keys

Available for Windows, Mac, and Linux

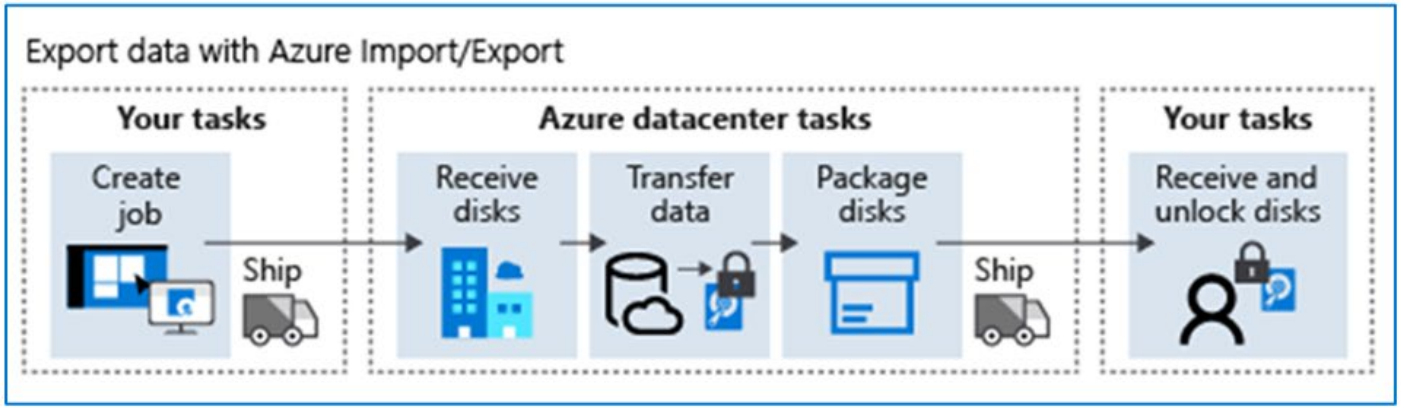


Import and Export Service

Import jobs move large amounts of data to Azure blob storage or files



Export jobs move large amounts of data from Azure Storage (not files)



AzCopy

```
azcopy copy [source] [destination] [flags]
```

Command line utility

Designed for copying data to and from Azure Blob, File, and Table storage

Available on Windows, Linux, and MacOS

Authentication options include Active Directory or SAS token

Microsoft Azure

Module 08:
Azure Virtual Machines

Module Overview

Lesson 01: Virtual Machine Planning

Lesson 02: Creating Virtual Machines

Lesson 03: Virtual Machine Availability

Lesson 04: Virtual Machine Extensions

Lesson 01: Virtual Machine Planning

Virtual Machine Planning Overview

IaaS Cloud Services

Virtual Machine Disks

Planning Checklist

Storage Options

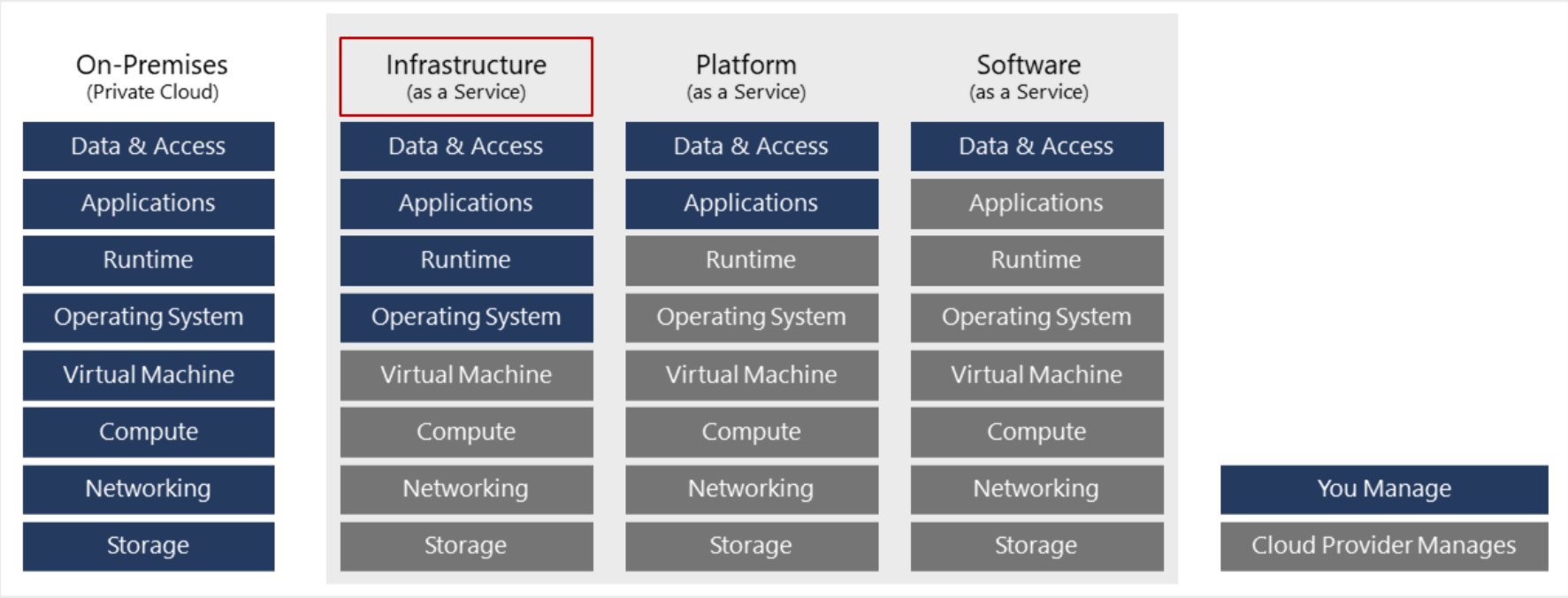
Location and Pricing

Supported Operating Systems

Virtual Machine Sizing

Virtual Machine Connections

IaaS Cloud Services



Test and development, website hosting, storage, backup, recovery,
high-performance computing, big data analysis, and extended data center

Planning Checklist

Start with the network

Understand the pricing model

Name the VM

Consider storage for the VM

Decide the location for the VM

Select an operating system

Determine the size of the VM

Location and Pricing

Location:

Each region has different hardware and service capabilities

Locate Virtual Machines as close as possible to your users

Locate Virtual Machines to ensure compliance and legal obligations

Pricing:

Compute costs

Storage costs (consumption-based and reserved instances)

60+ Azure regions
Available in 140 countries

Virtual Machine Sizing

A Series - Entry-level for dev/test

Bs Series – Economical bursting

D Series – General purpose compute

Dc Series – Protect data in use

E Series – In-memory hyper-threaded applications optimized

F Series – Compute optimized

G Series – Memory and storage optimized

H Series - High performance computing

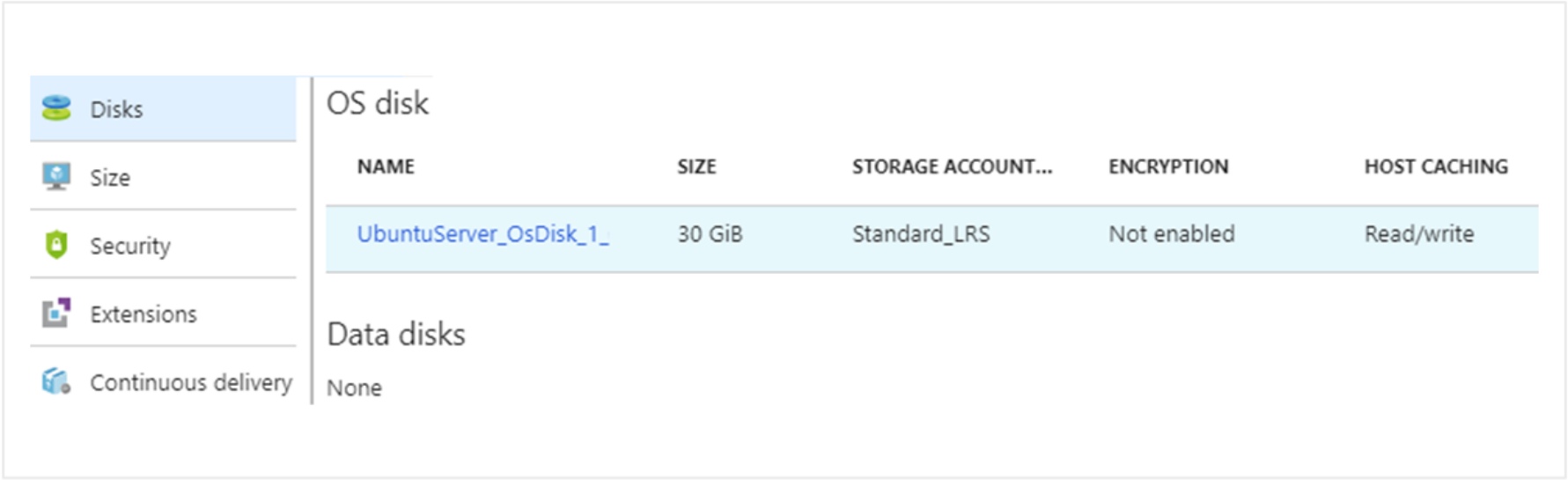
Ls Series – Storage optimized

M Series – Memory optimized

Mv2 Series – Largest memory optimized

N Series – GPU enabled

Virtual Machine Disks



Operating System Disks are SATA drives, labeled as C:

Temporary Disks provides short term storage

Data Disks are SCSI drives and depend on your virtual machine type

Storage Options

Premium storage offers high-performance, low-latency SSD disk support

Use premium storage for Virtual Machines with input/output (I/O)-intensive workloads

Two types of disks: Unmanaged and Managed:

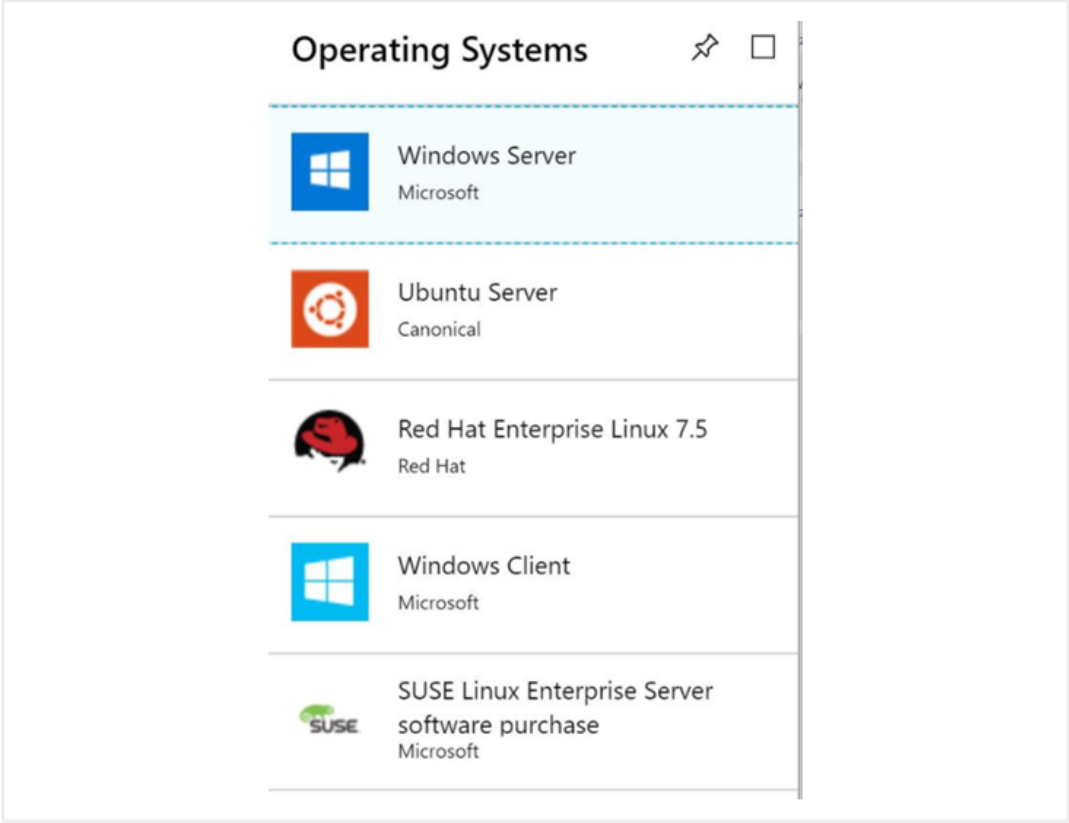
Unmanaged disks require you to manage the storage accounts and VHDs

Managed disks are maintained by Azure (recommended)

Supported Operating Systems

Windows Server includes many common products, requires a license, doesn't support OS upgrades

Linux distributions are supported, upgrade of the OS is supported

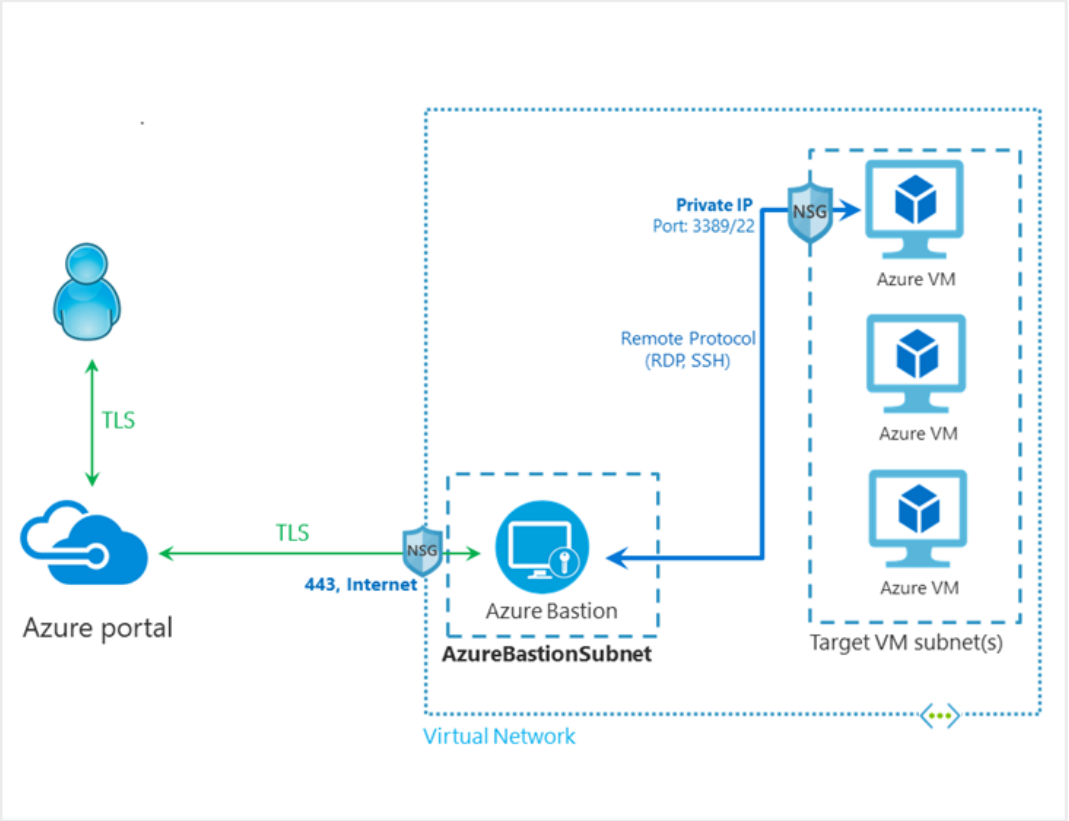


Virtual Machine Connections

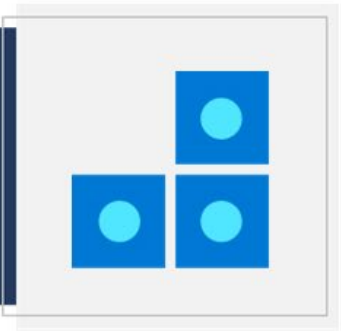
Remote Desktop Protocol for Windows-based Virtual Machines

Secure Shell Protocol for Linux based Virtual Machines

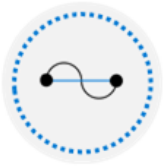
Bastion Subnet for RDP/SSH through the Portal over SSL



Lesson 02: Creating Virtual Machines



Creating Virtual Machines Overview



Creating Virtual Machines in the Portal

Linux Virtual Machines

Windows Virtual Machines

Linux VM Connections

Windows VM Connections

Creating Virtual Machines in the Portal

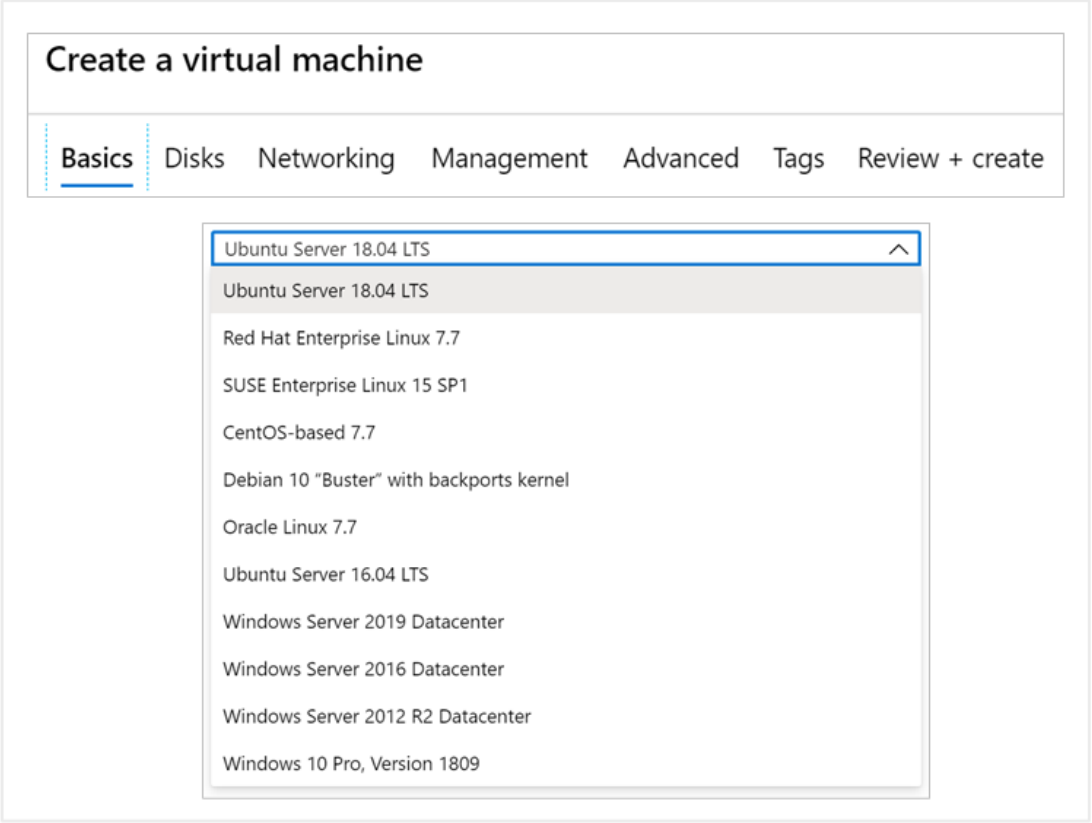
Basic (required) – Project details, Administrator account, Inbound port rules

Disks – OS disk type, data disks

Networking – Virtual networks, load balancing

Management – Monitoring, Auto-shutdown, Backup

Advanced – Add additional configuration, agents, scripts or applications



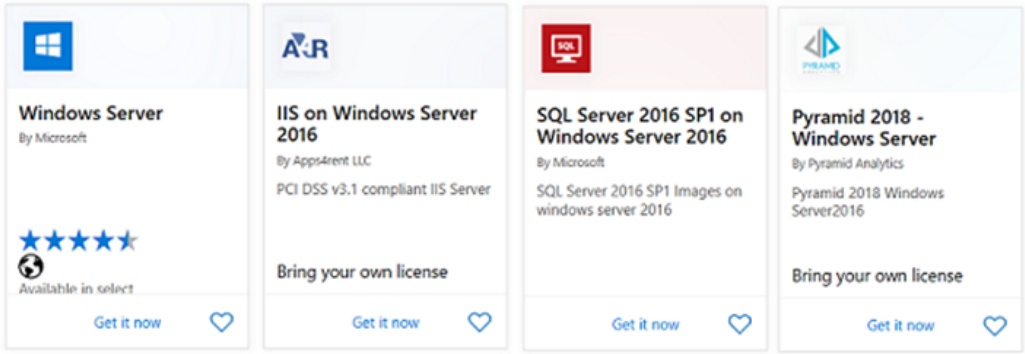
Windows Virtual Machines

Unique hybrid capabilities

Advanced multi-layer security

Faster innovation for applications

Unprecedented hyper-converged infrastructure

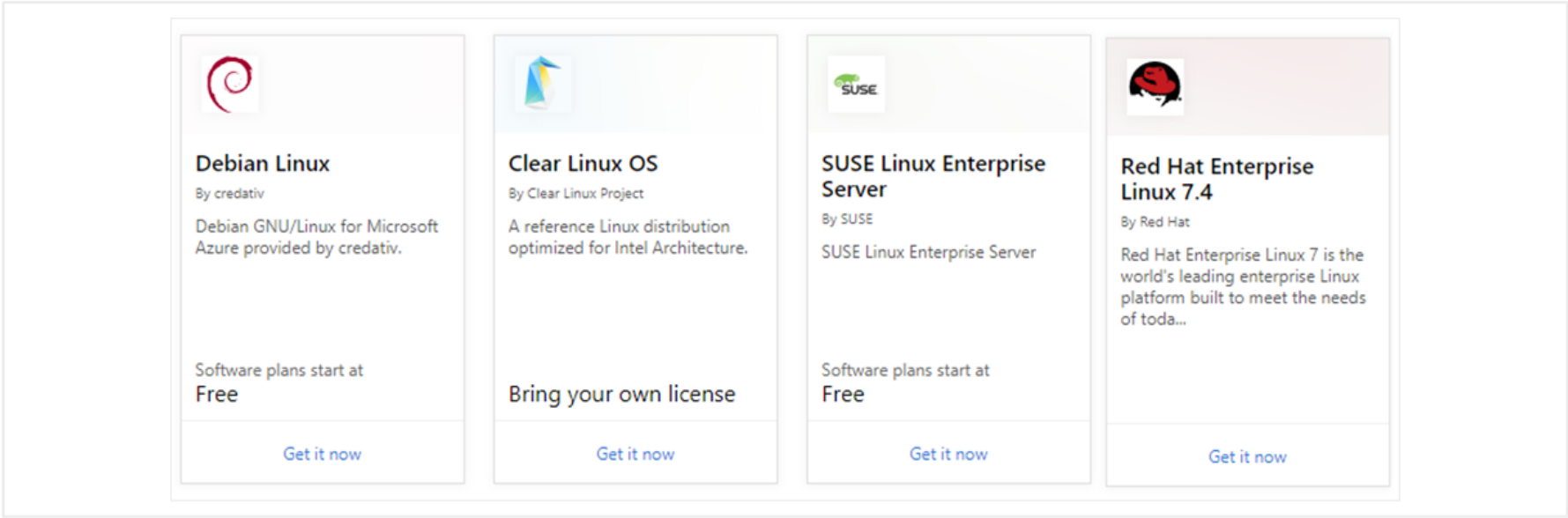


Windows VM Connections

Remote Desktop Protocol (RDP) creates a GUI session and accepts inbound traffic on TCP port 3389

WinRM creates a command-line session so can run scripts

Linux Virtual Machines

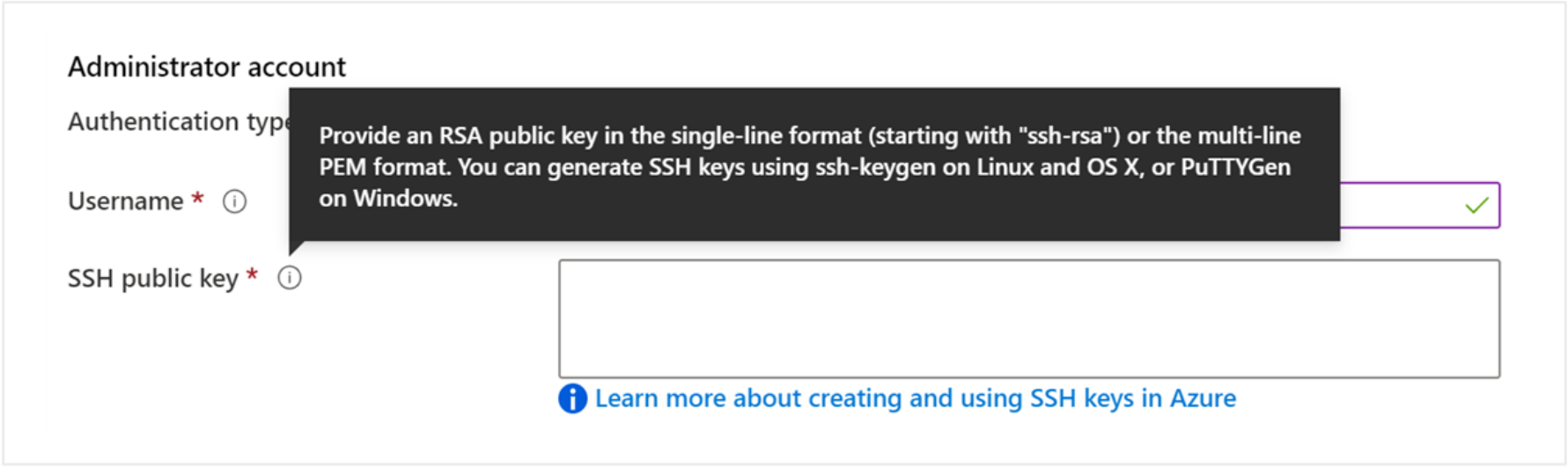


Hundreds of community-built images in the Azure Marketplace

Linux has the same deployment options as for Windows VMs

Manage Linux VMs with many popular open-source DevOps tools

Linux VM Connections



Authenticate with a SSH public key or password

SSH is an encrypted connection protocol that allows secure logins over unsecured connections

There are public and private keys

Lesson 03: Virtual Machine Availability

Virtual Machine Availability Overview

Maintenance and Downtime

Availability Sets

Update and Fault Domains

Availability Zones

Scaling Concepts

Scale Sets

Implementing Scale Sets

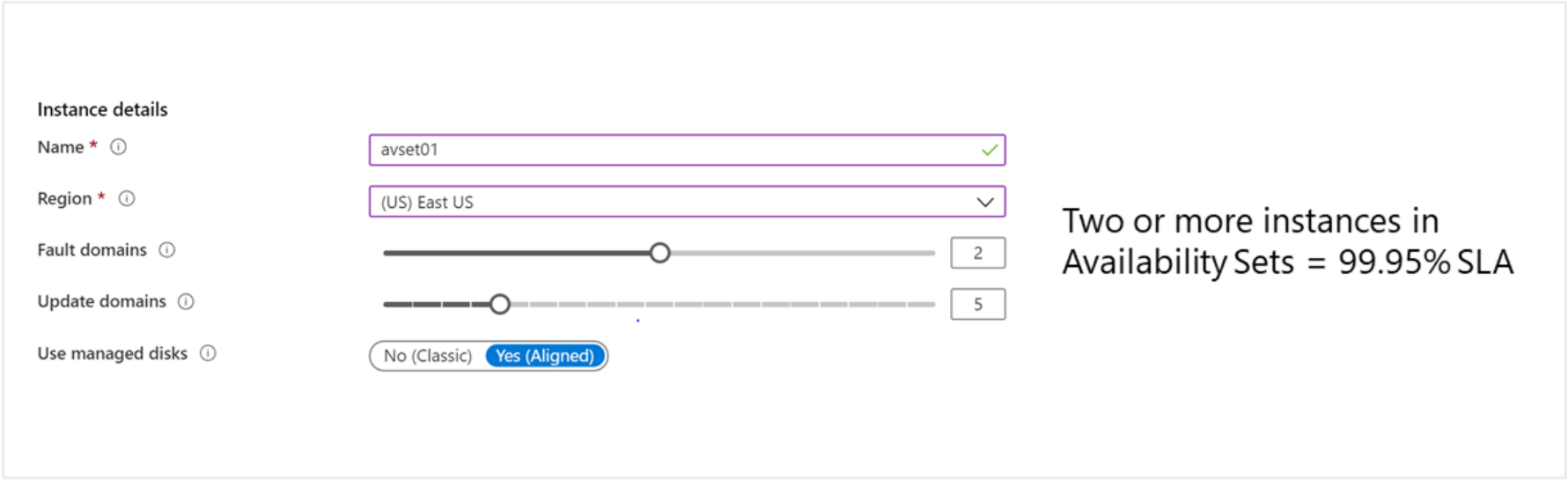
Autoscale

Implementing Autoscale

Maintenance vs. Downtime

Unplanned Hardware Maintenance	Unexpected Downtime	Planned Maintenance
When the platform predicts a failure, it will issue an **unplanned hardware maintenance** event **Action:** Live migration	**Unexpected Downtime** is when a virtual machine fails unexpectedly **Action:** Automatically migrate (heal)	**Planned Maintenance** events are periodic updates made to the Azure platform **Action:** No action

Availability Sets



Two or more instances in Availability Sets = 99.95% SLA

Configure multiple Virtual Machines in an Availability Set

Configure each application tier into separate Availability Sets

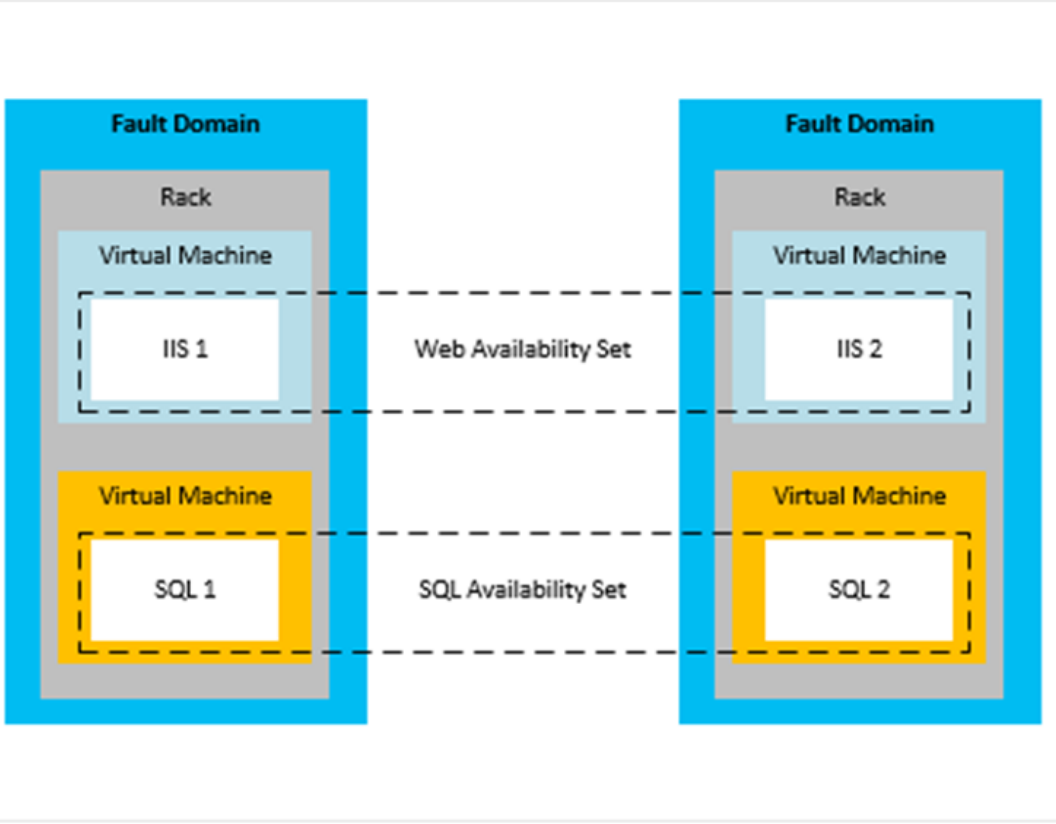
Combine a Load Balancer with Availability Sets

Use managed disks with the Virtual Machines

Update and Fault Domains

Update domains allows Azure to perform incremental or rolling upgrades across a deployment. During planned maintenance, only one update domain is rebooted at a time

Fault Domains are a group of Virtual Machines that share a common set of hardware, switches, that share a single point of failure. VMs in an availability set are placed in at least two fault domains



Availability Zones

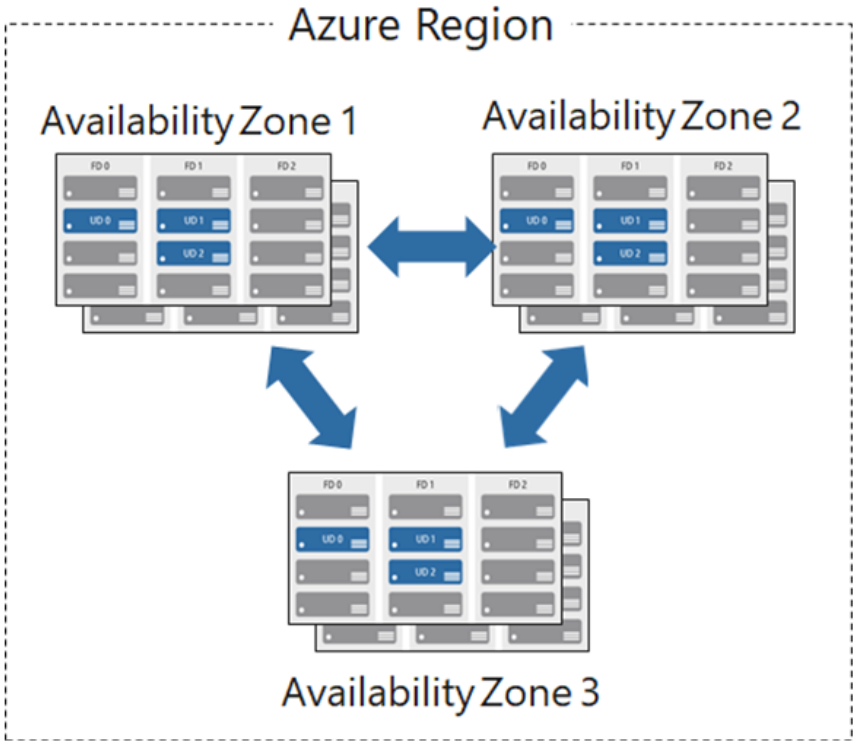
Unique physical locations in a region

Includes datacenters with independent power, cooling, and networking

Protects from datacenter failures

Combines update and fault domains

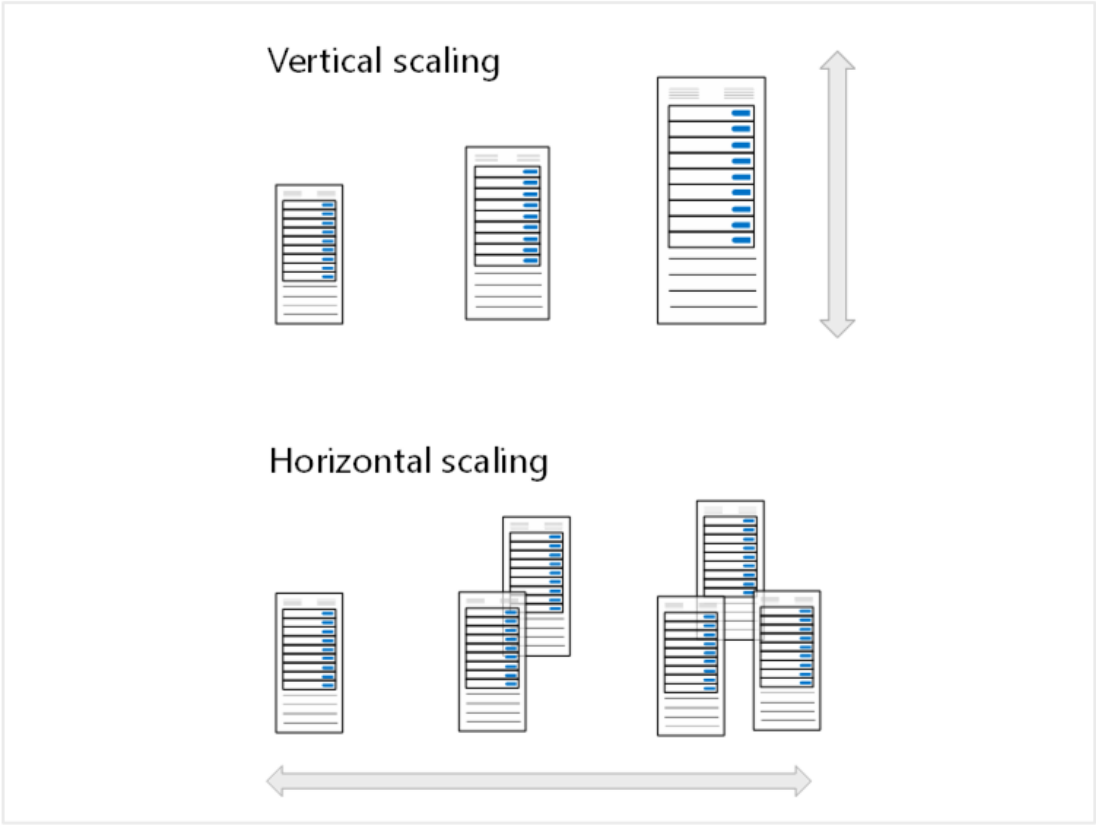
Provides 99.99% SLA



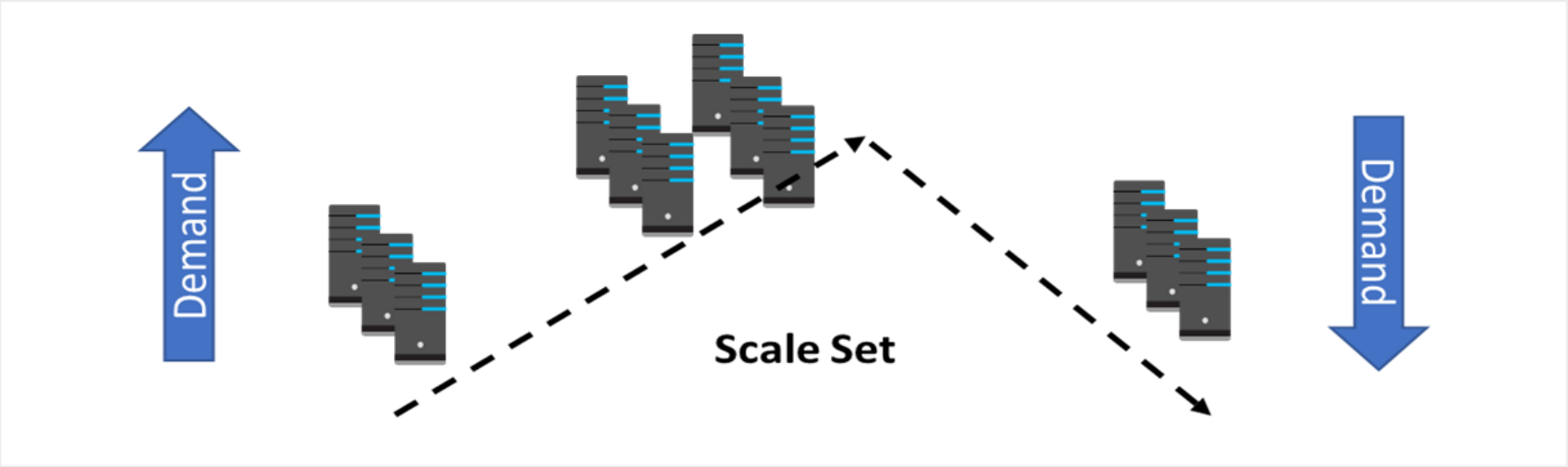
Scaling Concepts

Vertical scaling (scale up and scale down) is the process of increasing or decreasing power to a single instance of a workload; usually manual

Horizontal scaling (scale out and scale in) is the process of increasing or decreasing the number of instances of a workload; frequently automated



Scale Sets



Scale sets deploy a set of identical VMs	No pre-provisioning of VMs is required	As demand goes up VMs are added	As demand goes down VM are removed	The process can be manual, automated, or a combination of both

Implementing Scale Sets

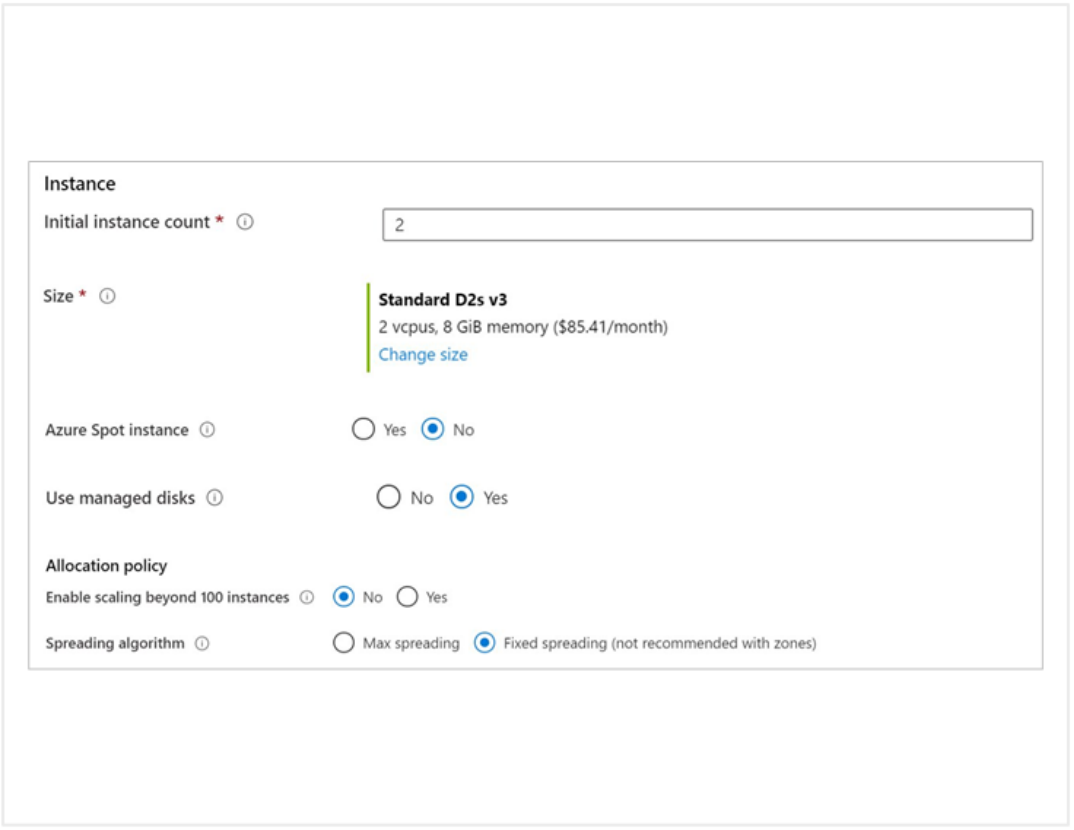
Instance count. Number of VMs in the scale set (0 to 1000)

Instance size. The size of each virtual machine in the scale set

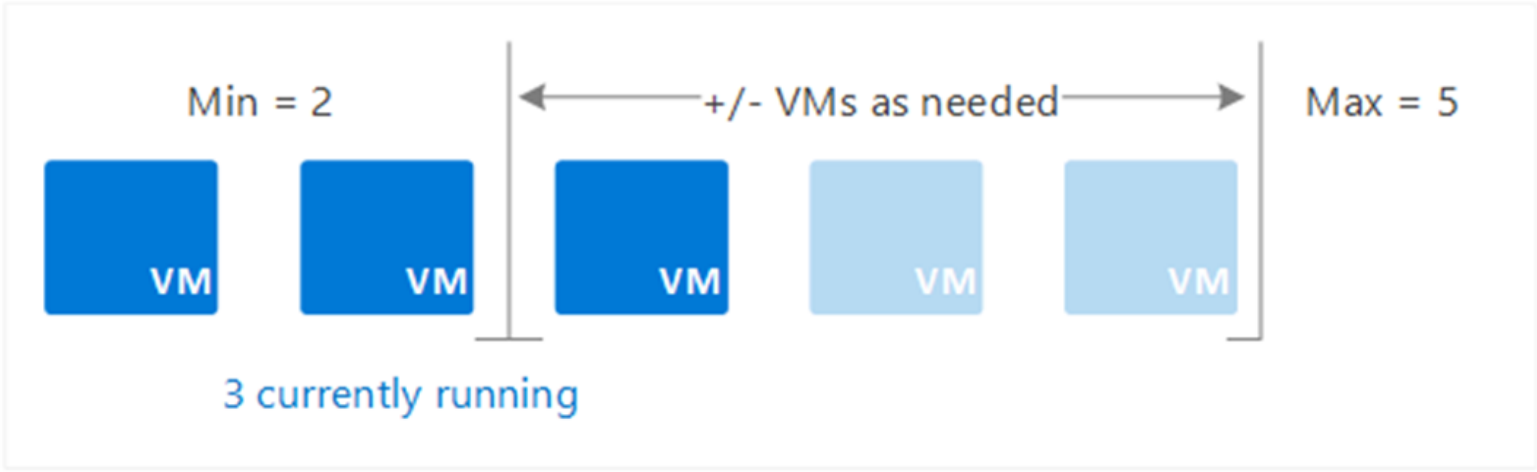
Azure Spot Instance. Unused capacity at a discounted rate

Use managed disks

Enable scaling beyond 100 instances



Autoscale

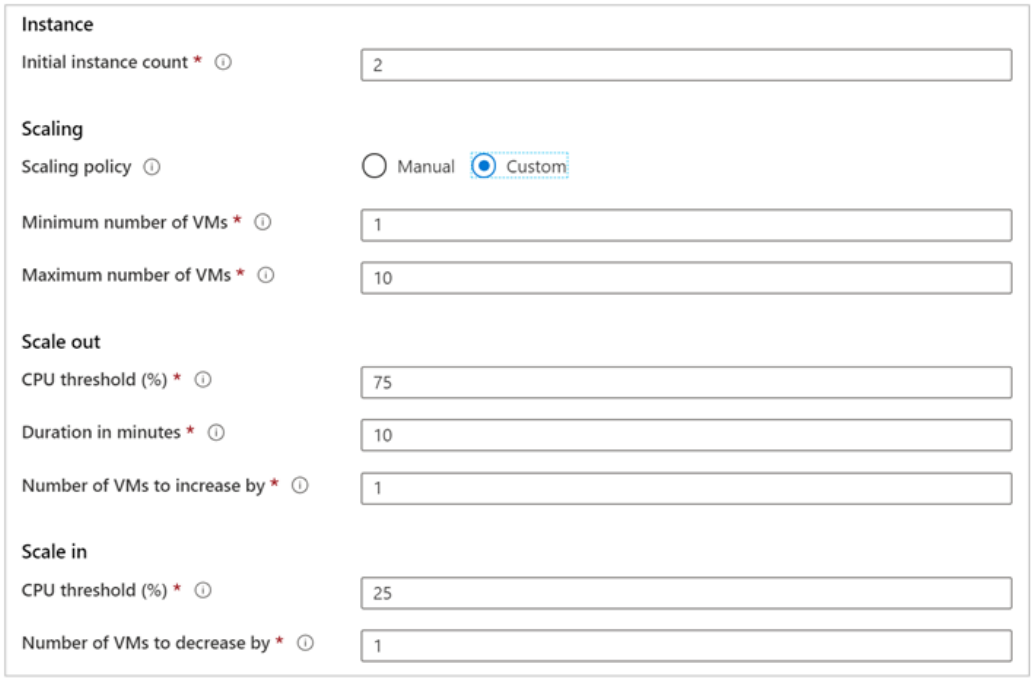


Define rules to automatically adjust capacity	Scale out (increase) the number of VMs in the set	Scale in (reduce) the number of VMs in the set	Schedule events to increase or decrease at a fixed time	Reduces monitoring and optimizes performance

Implementing Autoscale

Define a minimum, maximum, and default number of VM instances

Create more advanced scale sets with scale out and scale in parameters



Lesson 04: Virtual Machine Extensions

Virtual Machine Extensions Overview

Virtual Machine Extensions

Custom Script Extensions

Desired State Configuration

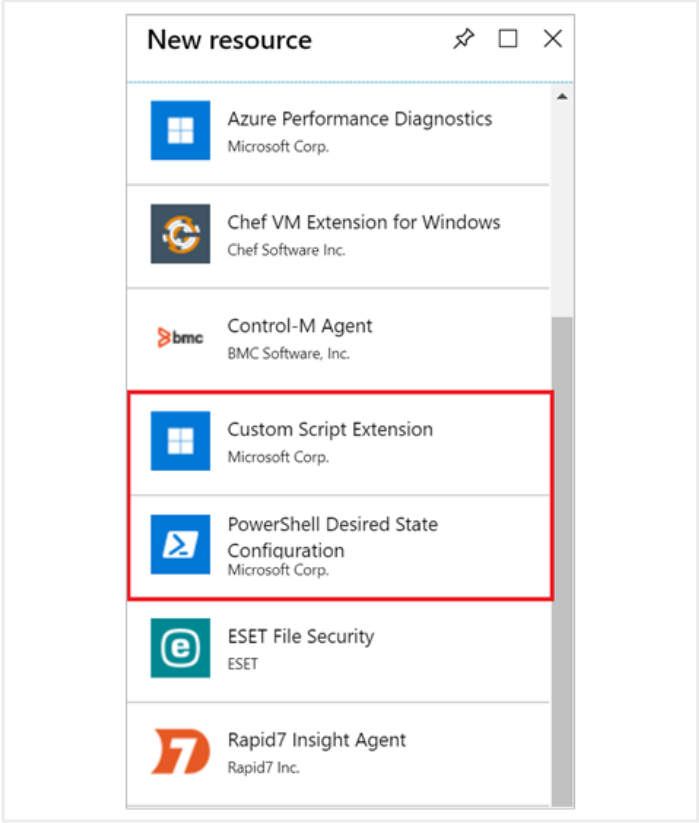
Virtual Machine Extensions

Extensions are small applications that provide post-deployment VM configuration and automation tasks

Managed with Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal

Bundled with a new VM deployment or run against any existing system

Different for Windows and Linux machines



Custom Script Extensions

Extension scripts can be simple or complex

Extensions have 90 minutes to run

Double check dependencies to ensure availability

Account for any errors that might occur

Protect/encrypt sensitive information

✓ For PowerShell use the Set-AzVmCustomScriptExtension command

Desired State Configuration

Configuration block(s) have a name

Node blocks define the computers or VMs that you are configuring

Resource block(s) configure the resource and its properties

There are many built-in configuration resources

```
configuration IISInstall
{
 Node “localhost”
 {
 WindowsFeature IIS
 {
 Ensure = “Present”
 Name = “Web-Server”
 }
 }
}
```

Microsoft Azure

Module 09: Monitoring

Module Overview

Lesson 01: Azure Monitor

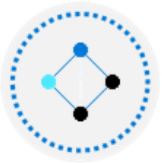
Lesson 02: Azure Alerts

Lesson 03: Log Analytics

Lesson 04: Network Watcher

Lesson 01: Azure Monitor

Azure Monitor Overview



Azure Monitor Service

Data Types

Key Capabilities

Azure Advisor

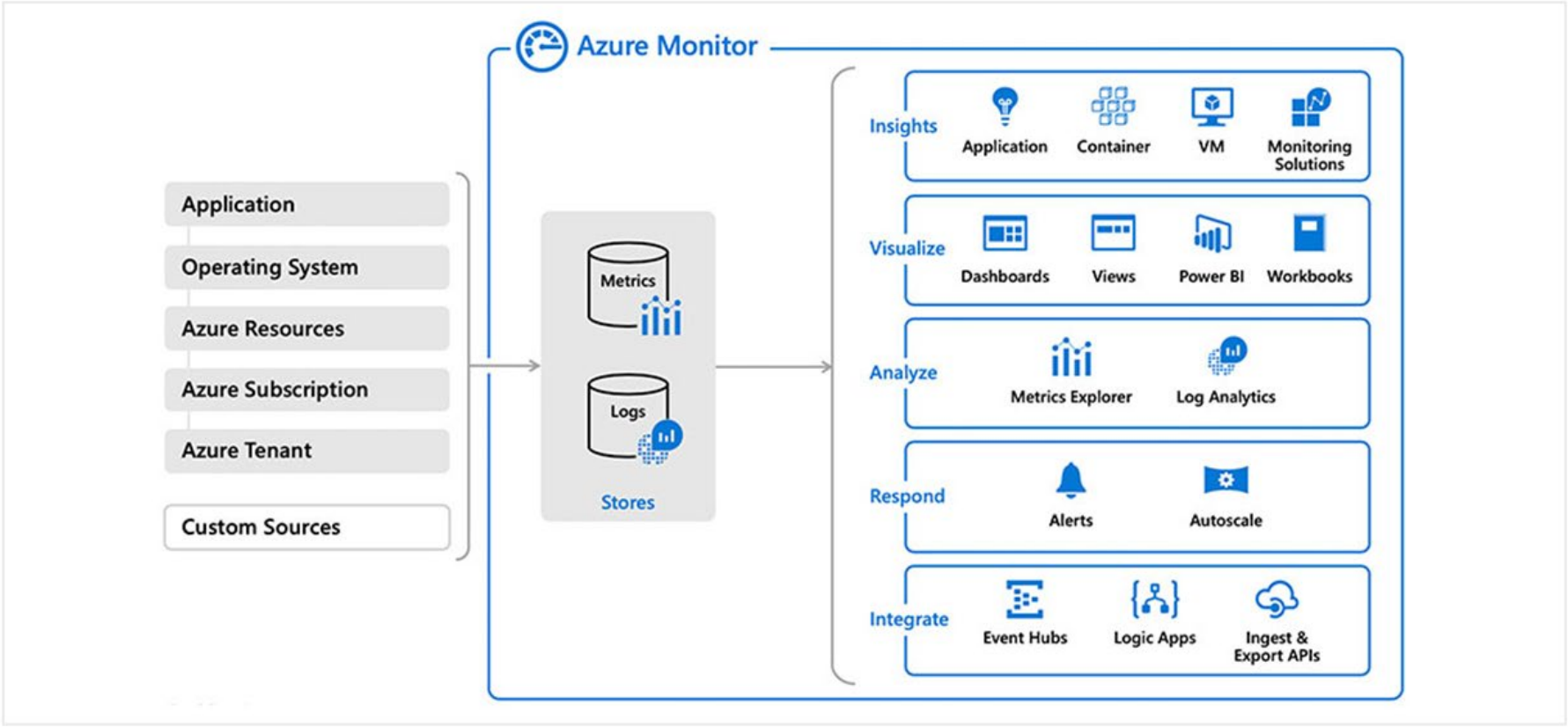
Monitoring Data Platform

Activity Log

Log Data

Query the Activity Log

Azure Monitor Service



Key Capabilities

Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

Explore Metrics

Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

Search Logs

Setup Alert & Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Create Alert

Core monitoring for Azure services

Collects metrics, activity logs, and diagnostic logs

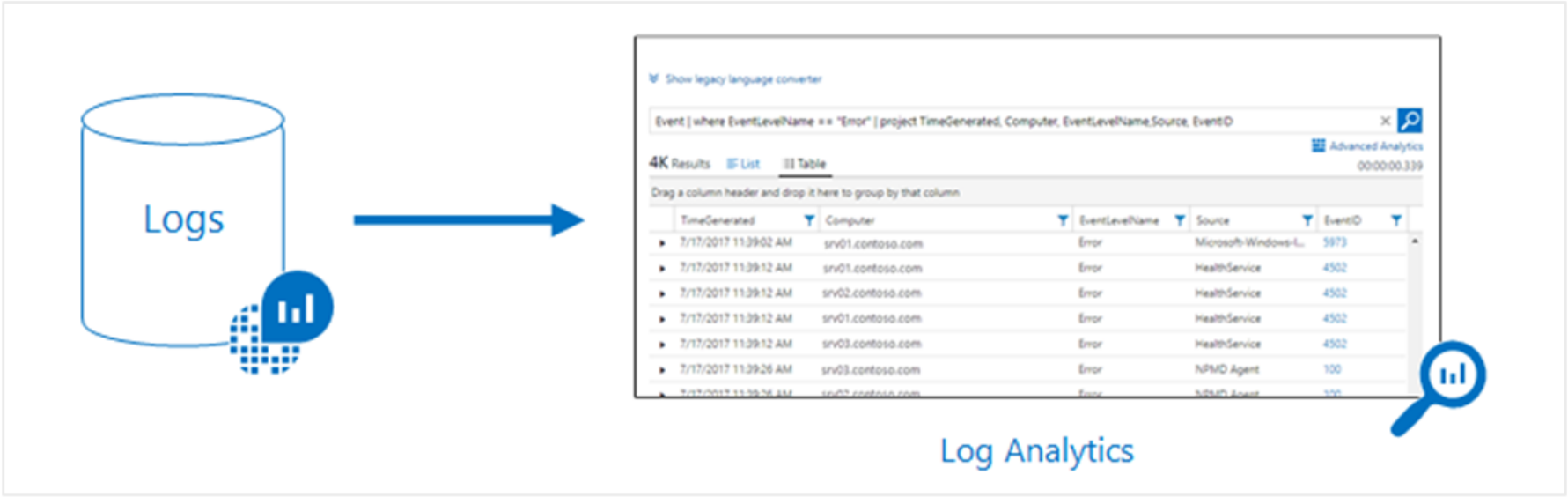
Use for time critical alerts and notifications

Monitoring Data Platform

Metrics are numerical values that describe some aspect of a system at a point in time. They are lightweight and capable of supporting near real-time scenarios

Logs contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis

Log Data



Log data is stored in Log Analytics which includes a rich query language to quickly retrieve, consolidate, and analyze collected data

The Data Explorer query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics

Data Types

Application monitoring data – Performance and functionality of the code you have written, regardless of its platform

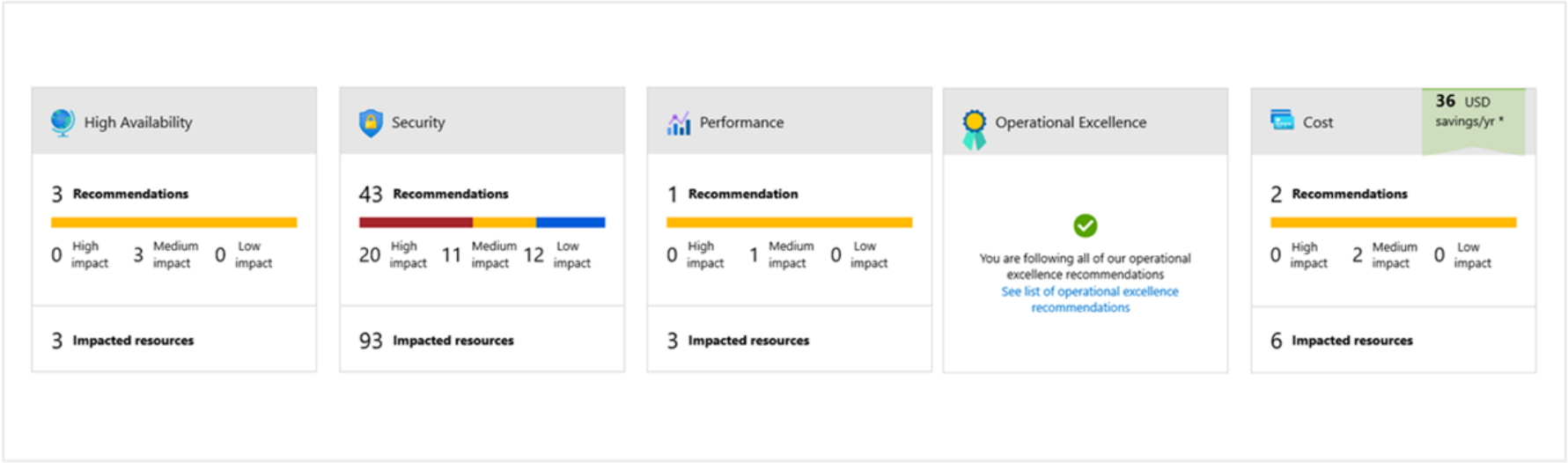
Guest OS monitoring – Azure, another cloud, or on-premises

Azure resource monitoring

Azure subscription monitoring – Operation and management of an Azure subscription, as well as data about the health and operation of Azure itself

Azure tenant monitoring – Operation of tenant-level Azure services, such as Azure Active Directory

Azure Advisor



Personalized cloud consultant

Analyzes your configuration and recommends solutions

High Availability, Security, Performance, Operational Excellence, and Cost

Activity Log

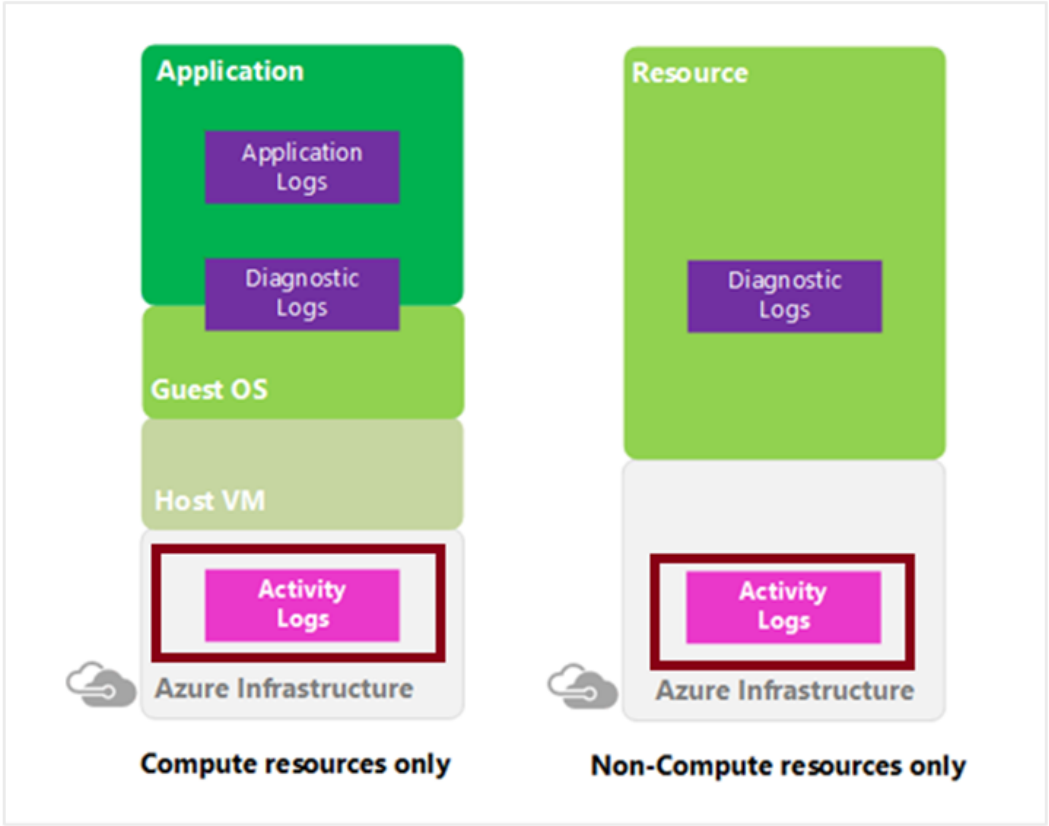
Send data to Log Analytics for advanced search and alerts

Query or manage events in the Portal, PowerShell, CLI, and REST API

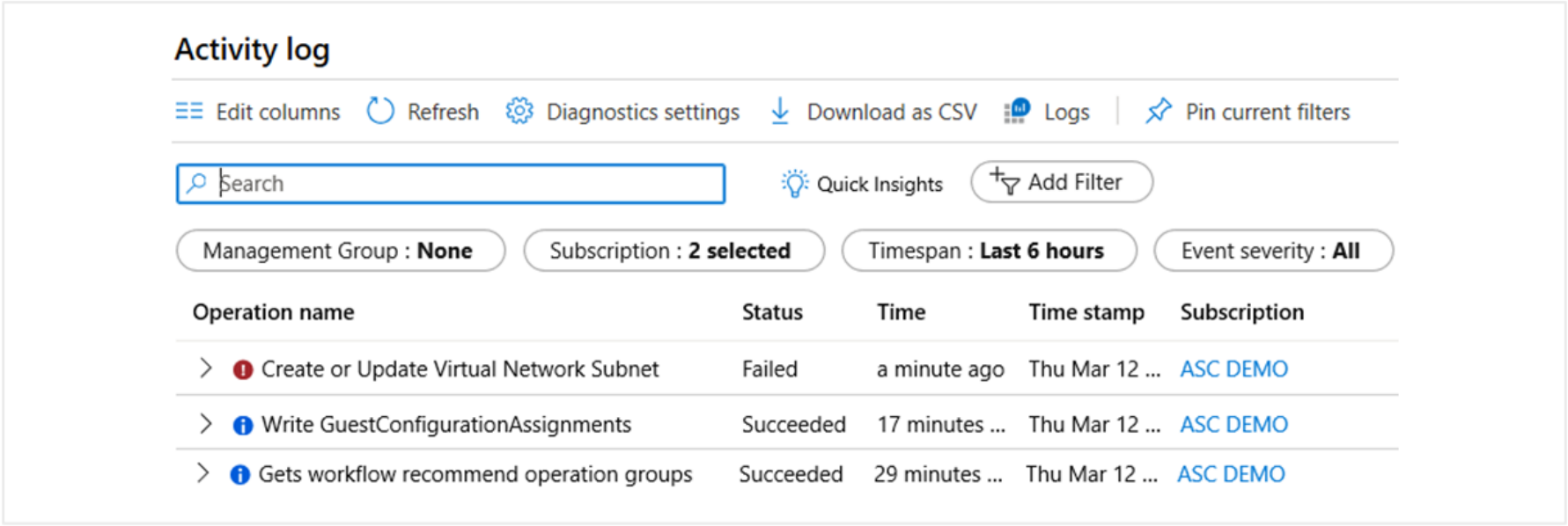
Stream information to Event Hub

Archive data to a storage account

Analyze data with Power BI



Query the Activity Log



Filter by Management group, Subscription, Timespan, and Event Severity

Add a filter, like Event Category (Security, Recommendations, Alerts)

Pin current filters and download as CSV

Lesson 02: Azure Alerts

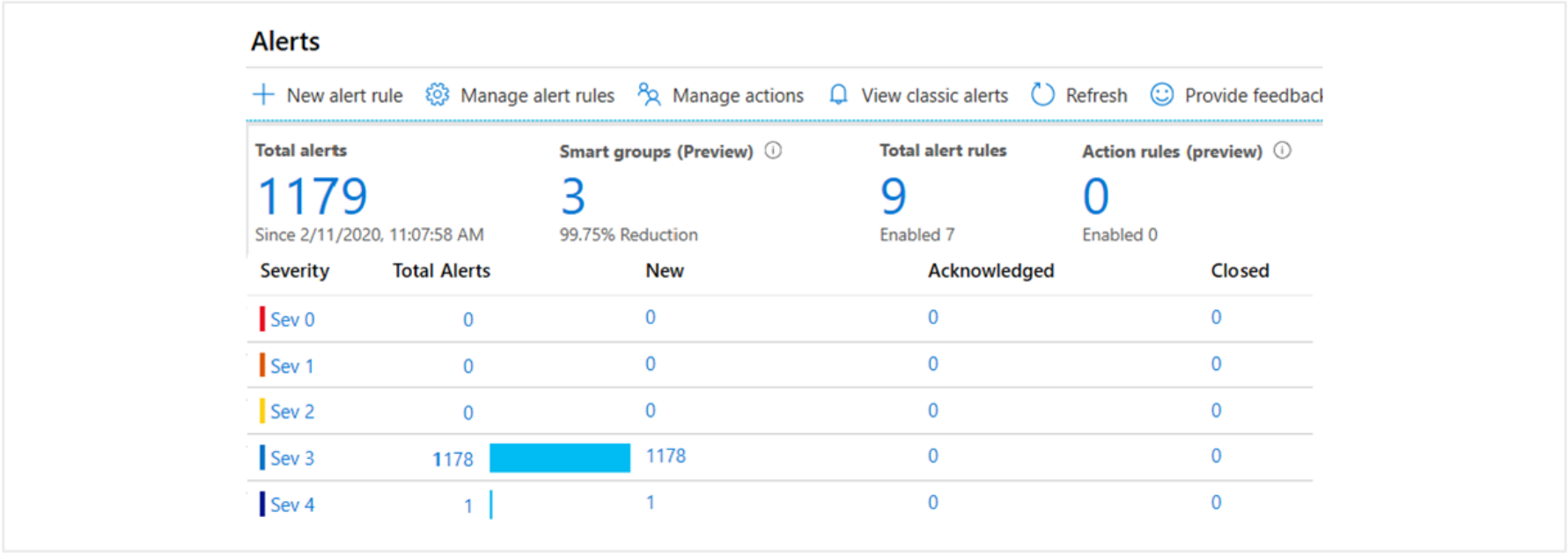
Azure Alerts Overview

Azure Monitor Alerts

Creating Alert Rules

Action Groups

Azure Monitor Alerts



Unified authoring experience

Displayed by severity

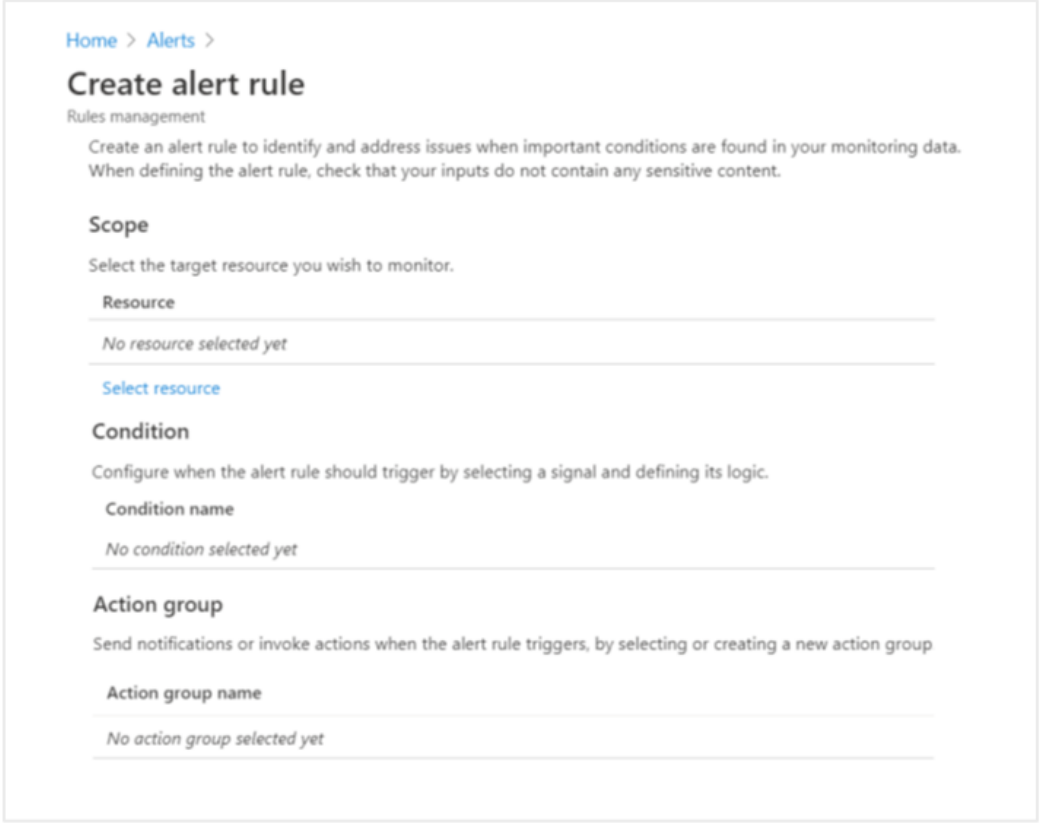
Categorized by New, Acknowledged, and Closed

Creating Alert Rules

Scope: Target selection, Alert criteria, and Alert logic

Condition: Alert rule name, description, and severity (0 to 4)

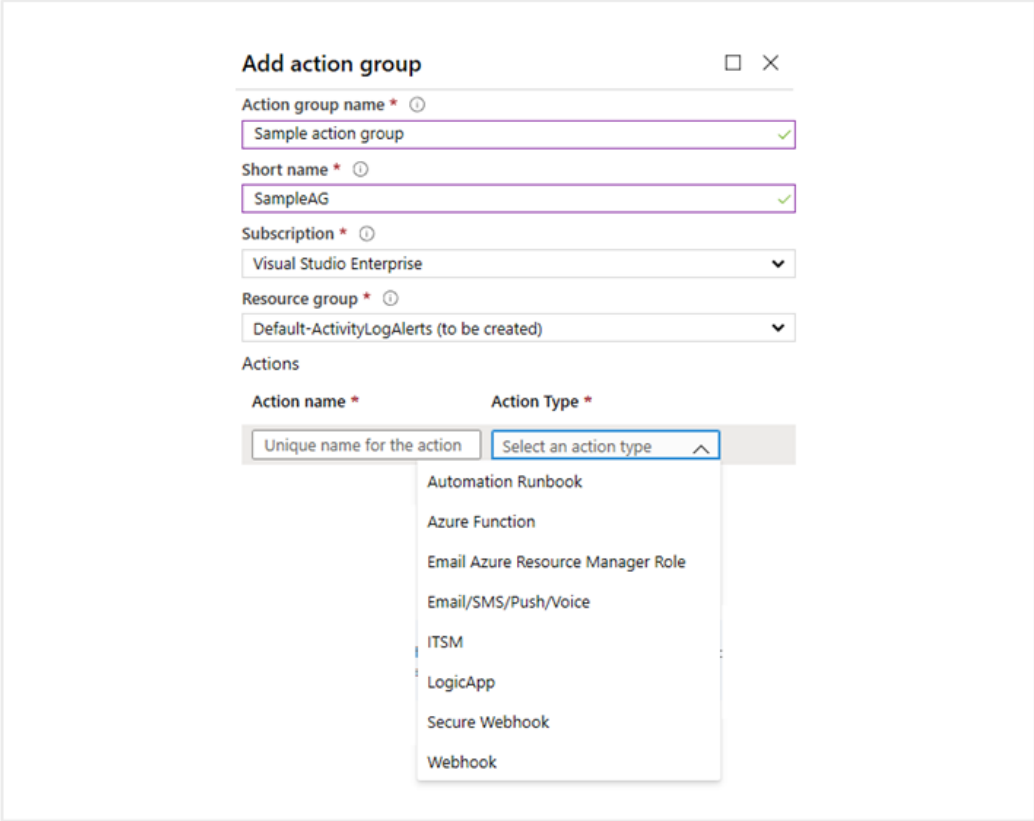
Action group: Notify your team via email and text messages or automate actions using webhooks and runbooks



Action Groups

Notifies a group of users that an alert has been triggered

Is a collection of notification preferences



Lesson 03: Log Analytics

Log Analytics Overview

Log Analytics

Create a Workspace

Connected Sources

Data Sources

Log Analytics Querying

Query Language Syntax

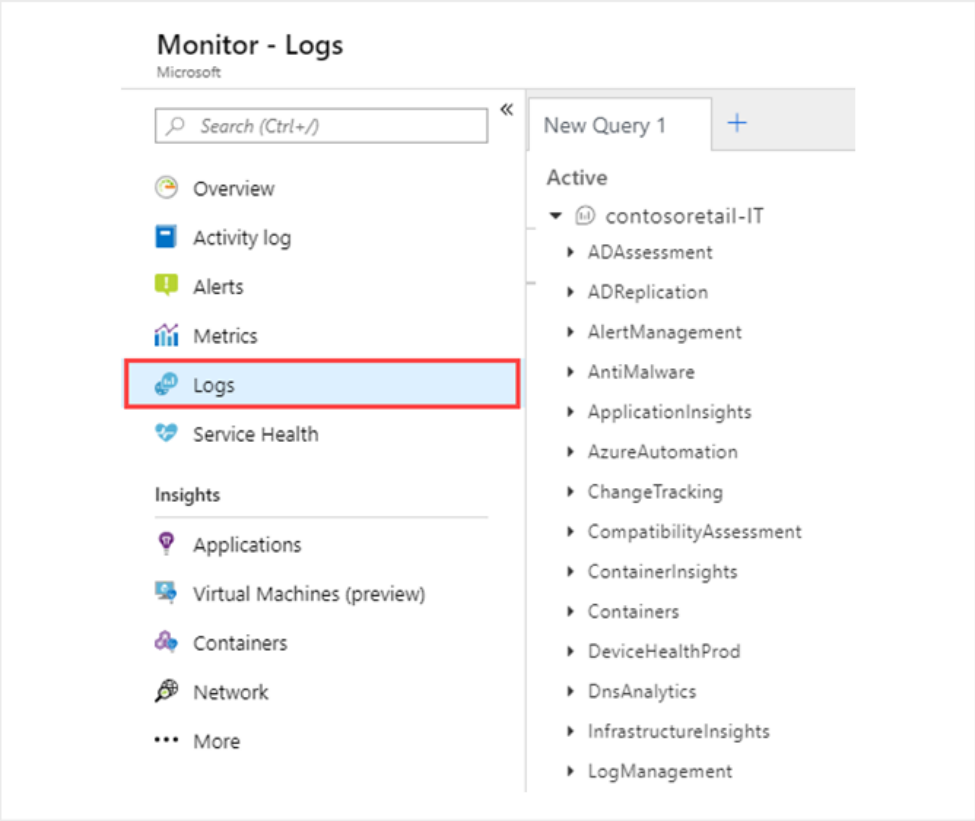
Demonstration – Log Analytics

Log Analytics

A service that helps you collect and analyze data generated by resources in your cloud and on-premises environments

Write log queries and interactively analyze their results

Examples include assessing system updates and troubleshooting operational incidents

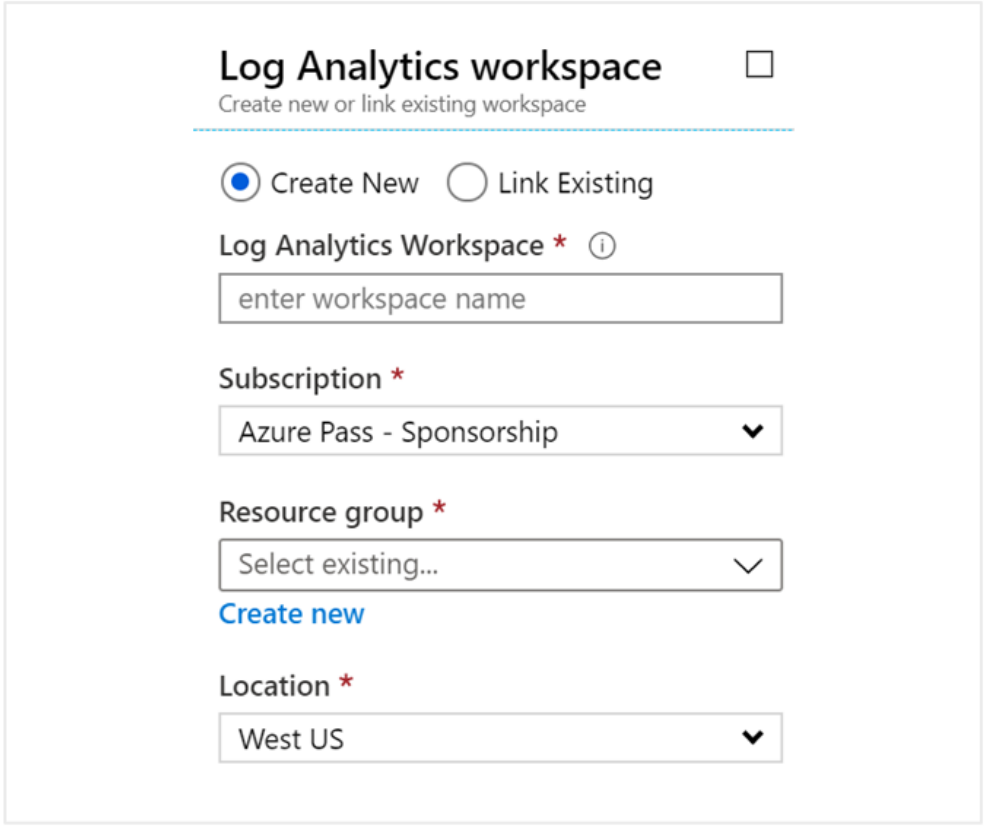


Create a Workspace

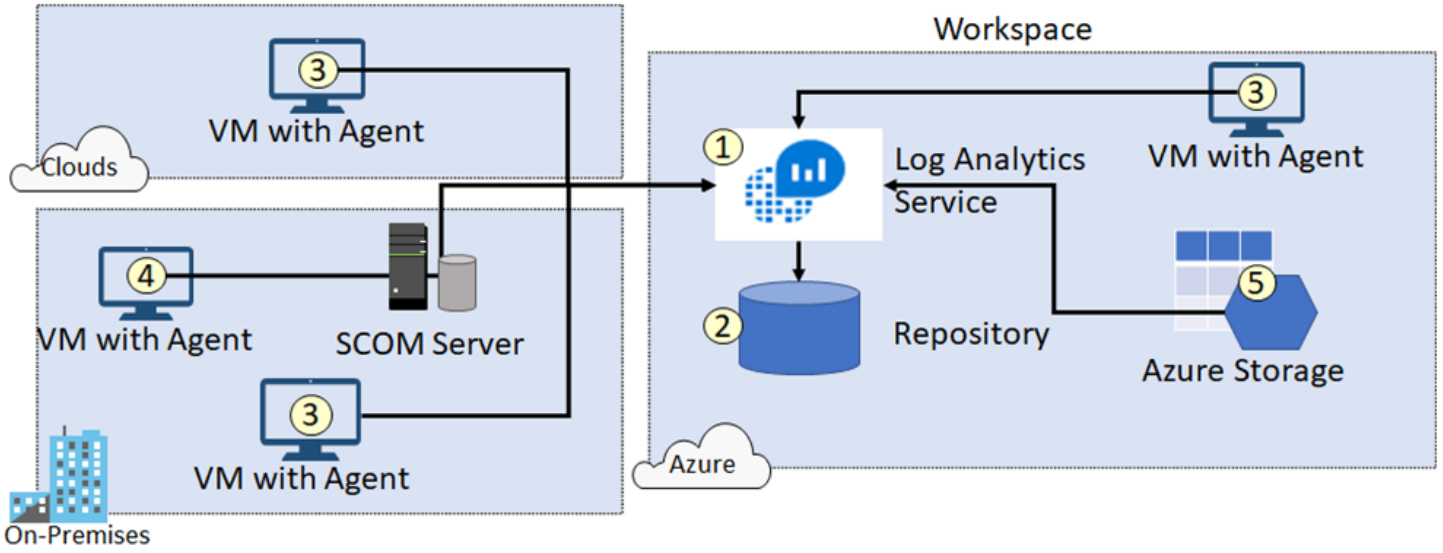
A workspace is an Azure resource and is a container where data is collected, aggregated, analyzed, and presented

You can have multiple workspaces per Azure subscription, and you can have access to more than one workspace

A workspace provides a geographic location, data isolation, and scope



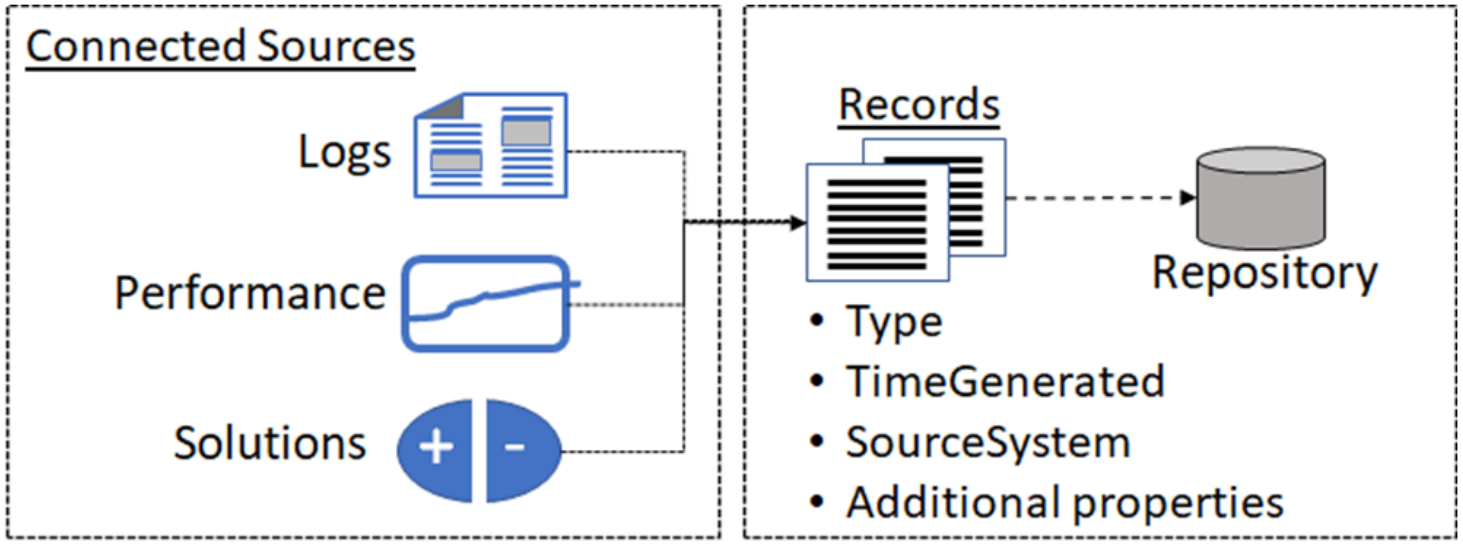
Connected Sources



Connected Sources generate data

Data can be collected from Windows, Linux, SCOM and Azure Storage

Data Sources



Data sources include: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog

Each data source has additional configuration options

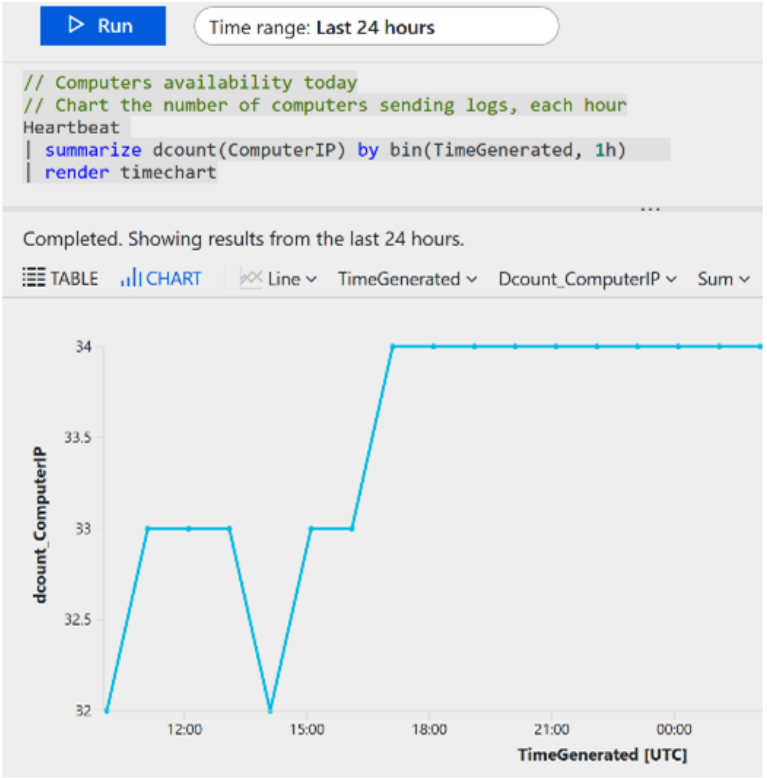
Log Analytics Querying

Log Analytics provides a query syntax

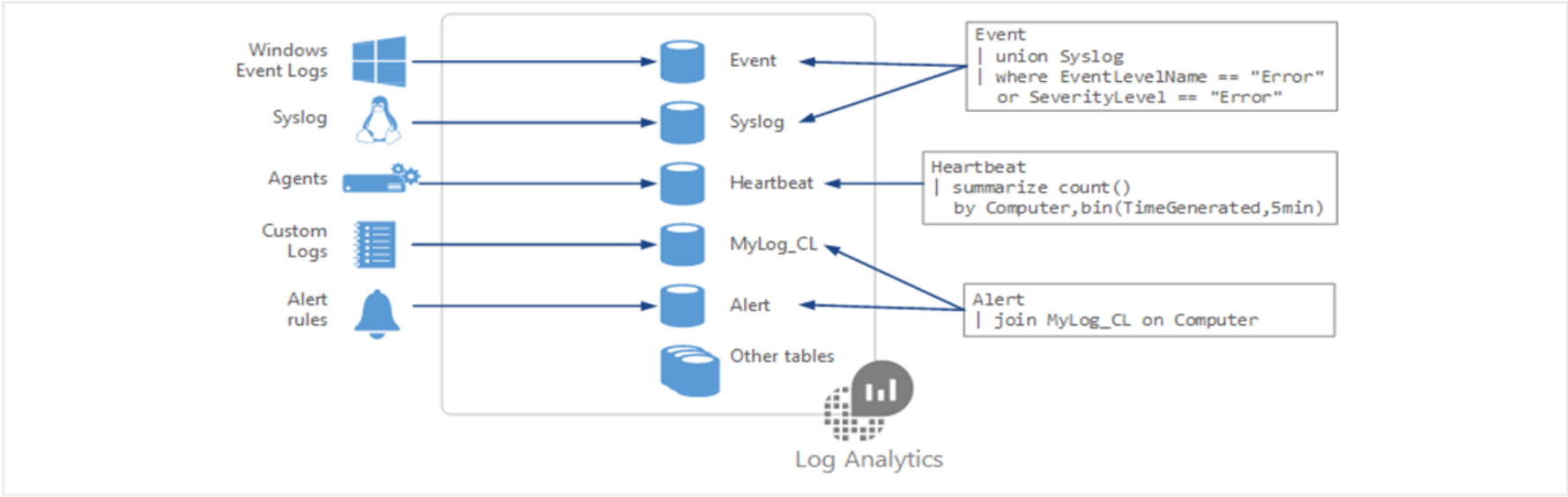
Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

Export the data to Power BI or Excel



Query Language Syntax




```
Event
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCount = count() by Computer
| top 10 by ErrorCount desc
```

Lesson 04: Network Watcher

Network Watcher Overview

Network Watcher

Network Watcher Diagnostics

Diagnostics – IP Flow Verify

Diagnostics – Next Hop

Diagnostics – Effective Security Rules

Diagnostics – VPN Troubleshoot

Diagnostics – Packet Capture

Diagnostics – Connection Troubleshoot

Logs – NSG Flow logs

Monitoring – Topology

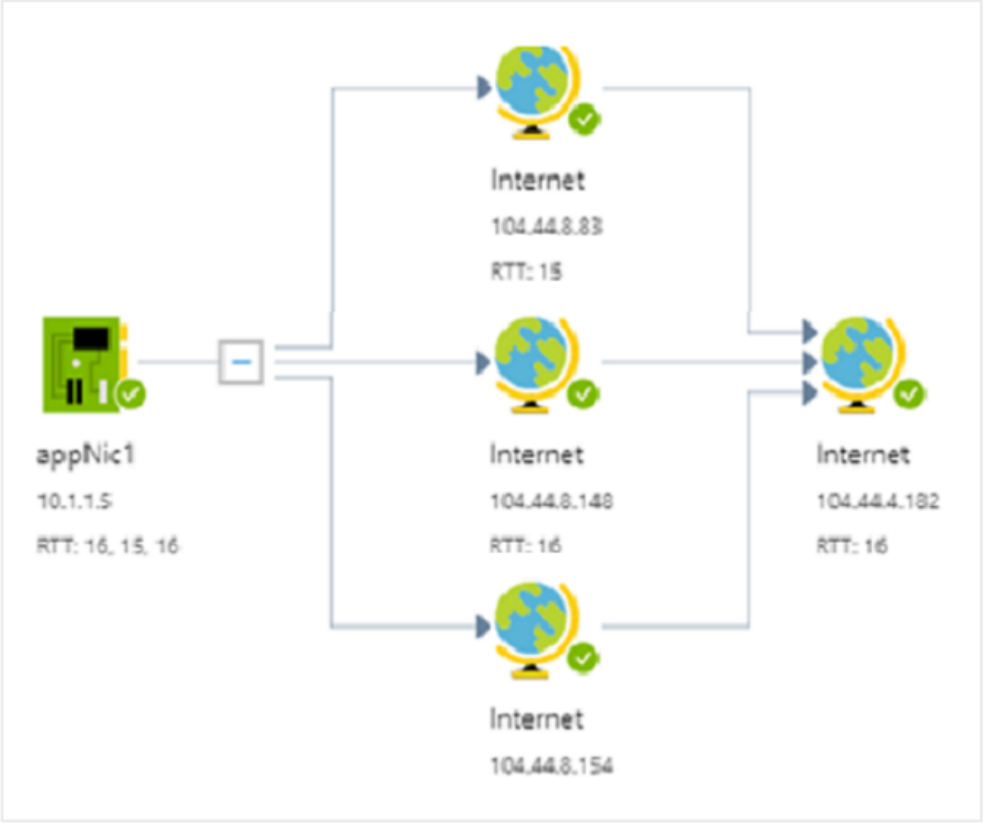
Network Watcher

Is a regional service

Provides tools to monitor, diagnose, view metrics, and enable or disable logs

Provides scenario level monitoring so you can diagnose problems at an end to end network level view

Provides a visual representation of your networking elements



Network Watcher Diagnostics

IP Flow Verify diagnoses connectivity issues

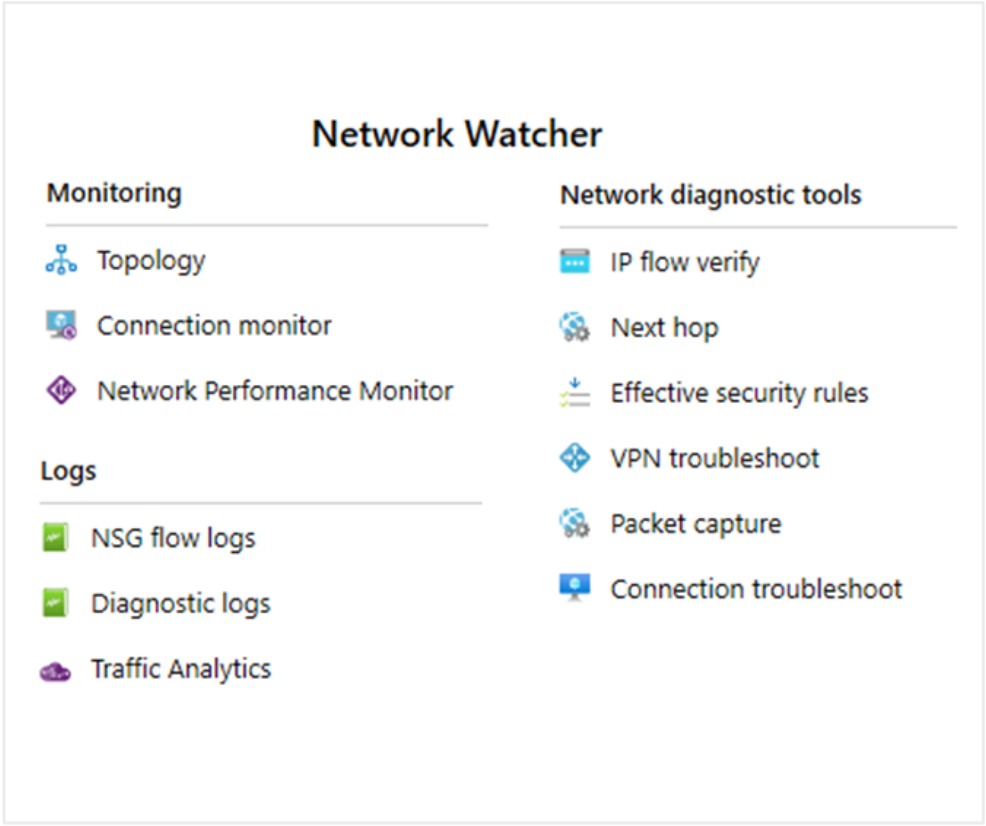
Next Hop determines if traffic is being correctly routed

VPN Diagnostics troubleshoots gateways and connections

NSG Flow Logs maps IP traffic through a network security group

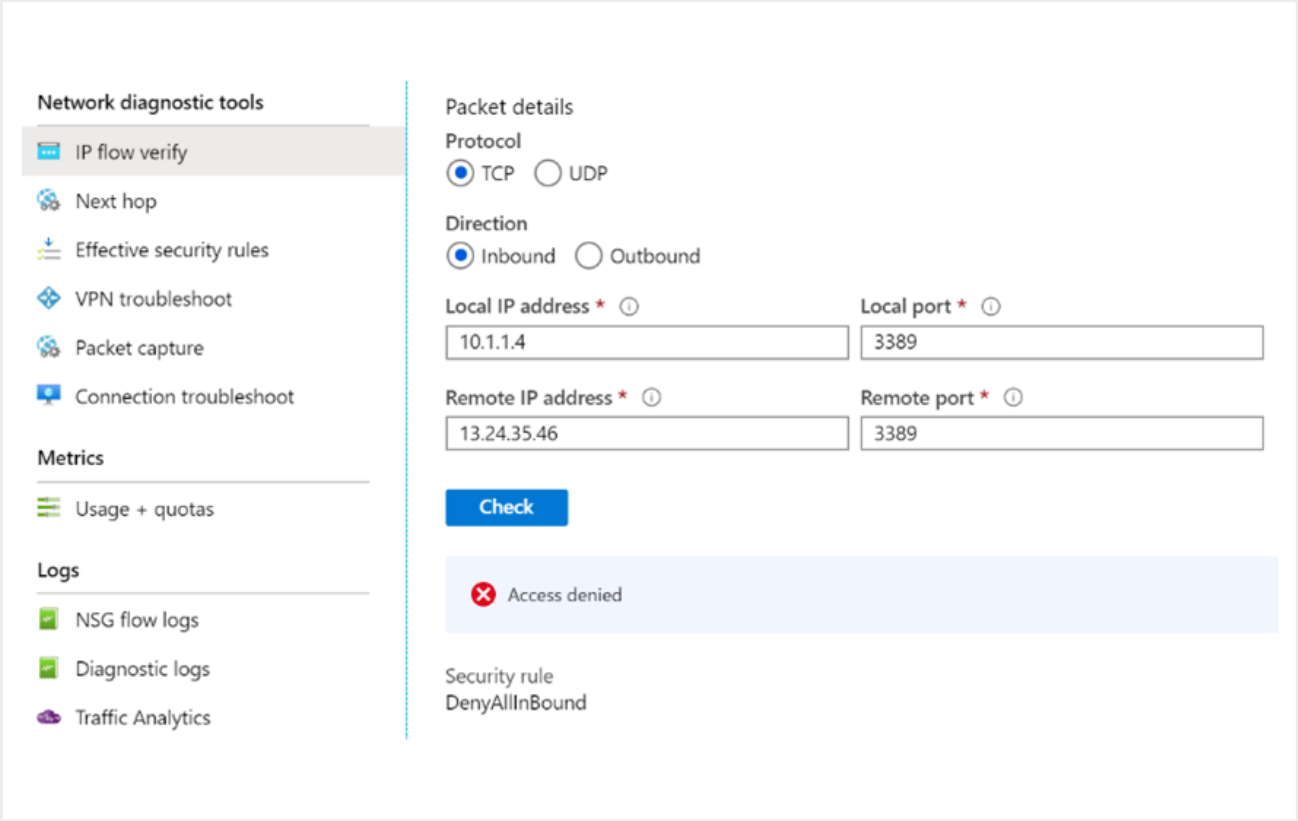
Connection troubleshoot shows connectivity between source VM and destination

Topology generates a visual diagram of resources



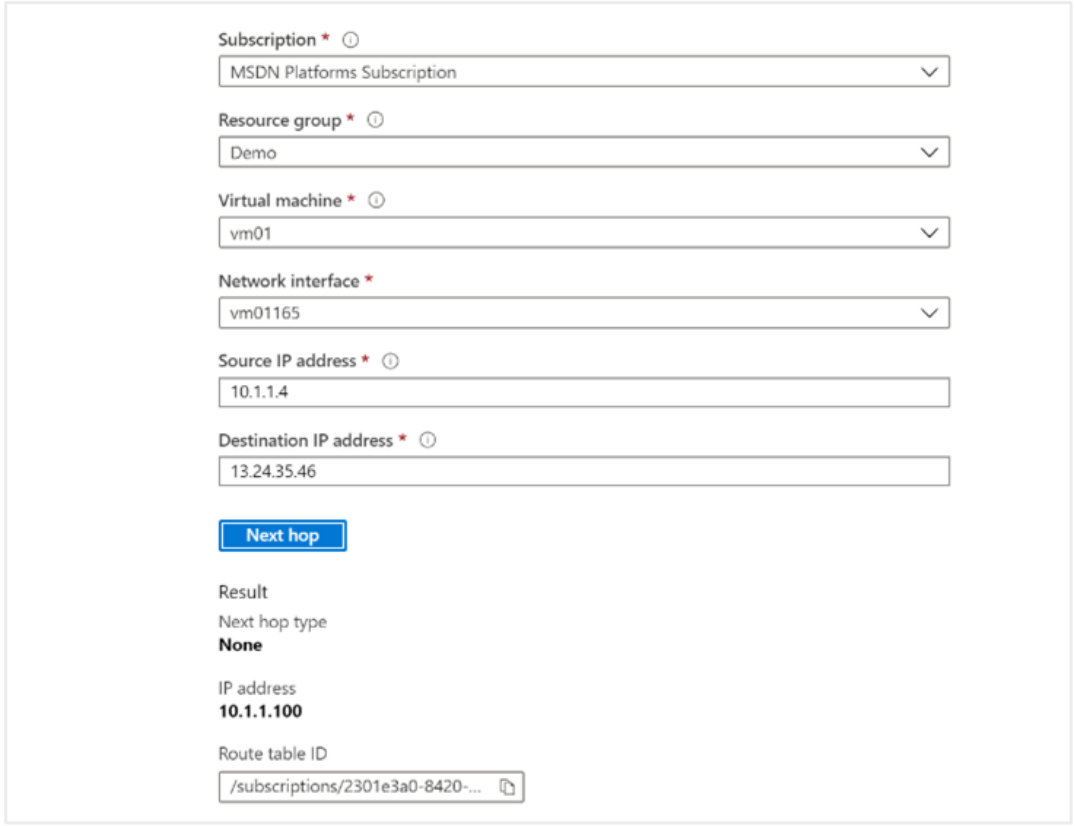
Diagnostics – IP Flow Verify

Diagnose connectivity issues from or to the internet and from or to the on-premises environment. Ideal for ensuring security rules are being correctly applied



Diagnostics – Next Hop

Helps with determining whether traffic is being directed to the intended destination by showing the next hop



Diagnostics – Effective Security Rules

nsg01

Inbound rules

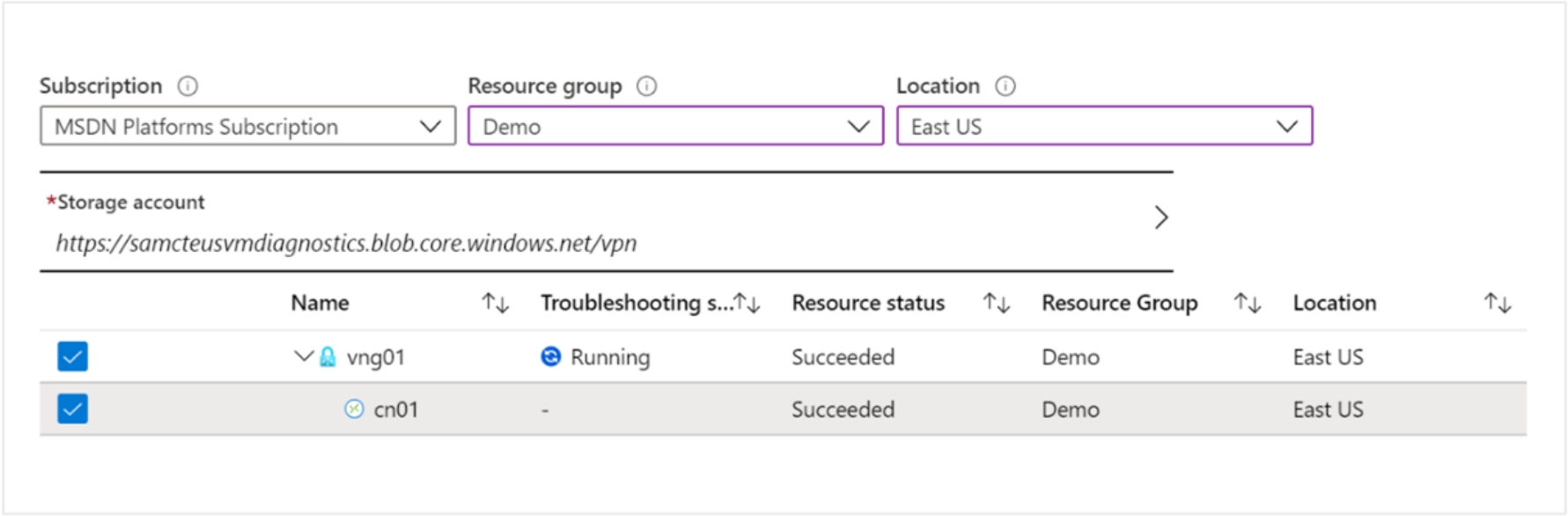
Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
RDP_Inbound	100	13.23.34.45/32	0-65535	0.0.0.0/0	3389-3389	TCP	Allow
AllowVnetInBound	65000	Virtual network (1 prefixes)	0-65535	Virtual network (1 prefixes)	0-65535	All	Allow
AllowAzureLoadBalancerInBound	65001	Azure load balancer (2 prefixes)	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Allow
DenyAllInBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Outbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
AllowVnetOutBound	65000	Virtual network (1 prefixes)	0-65535	Virtual network (1 prefixes)	0-65535	All	Allow
AllowInternetOutBound	65001	0.0.0.0/0,0.0.0.0/0	0-65535	Internet (216 prefixes)	0-65535	All	Allow
DenyAllOutBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Details the Effective Security Rules (inbound and outbound) of the Network Interface card of a Virtual Machine

Diagnostics – VPN Troubleshoot



Helps you troubleshoot gateways and connections

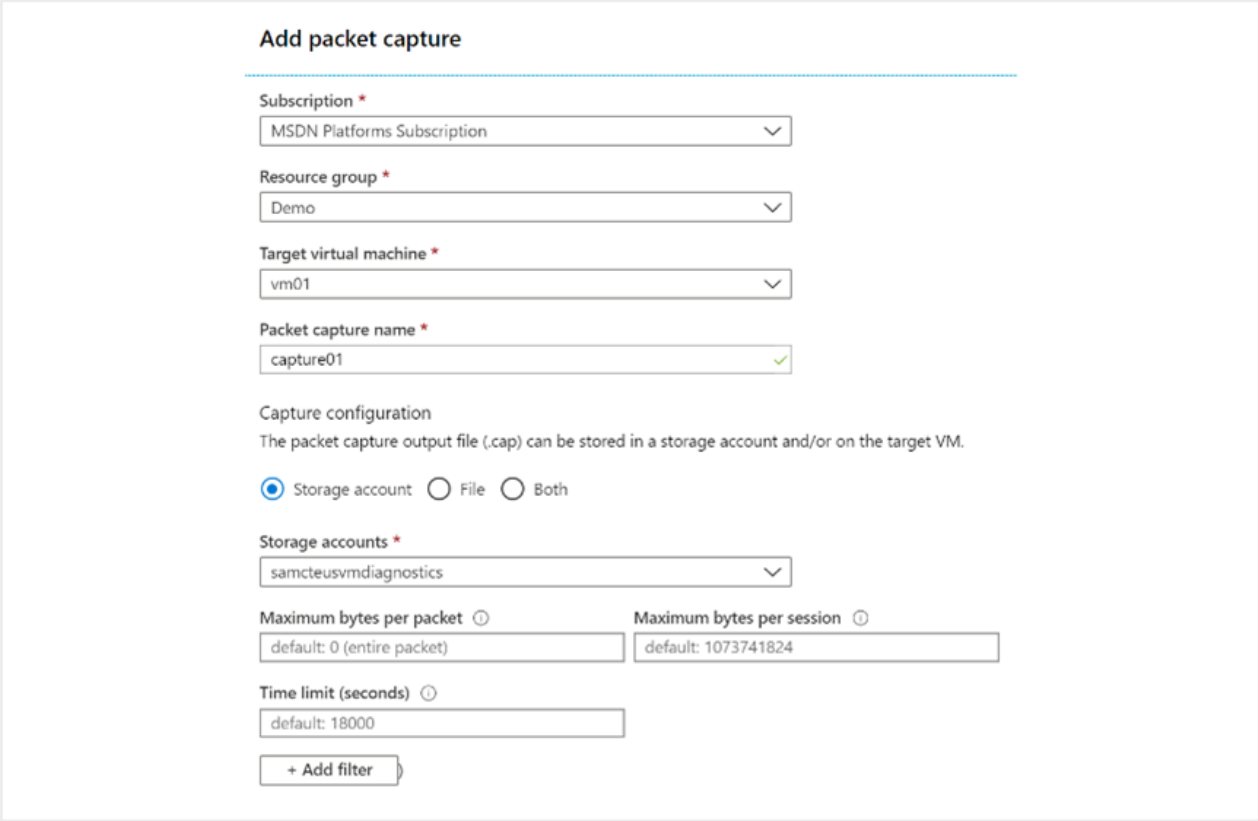
Provides summary information and detailed information

Can troubleshoot multiple gateways or connections simultaneously

Diagnostics – Packet Capture

Captures inbound and outbound traffic from a Virtual Machine

Saves data to a storage account, a local file, or both



Diagnostics – Connection Troubleshoot

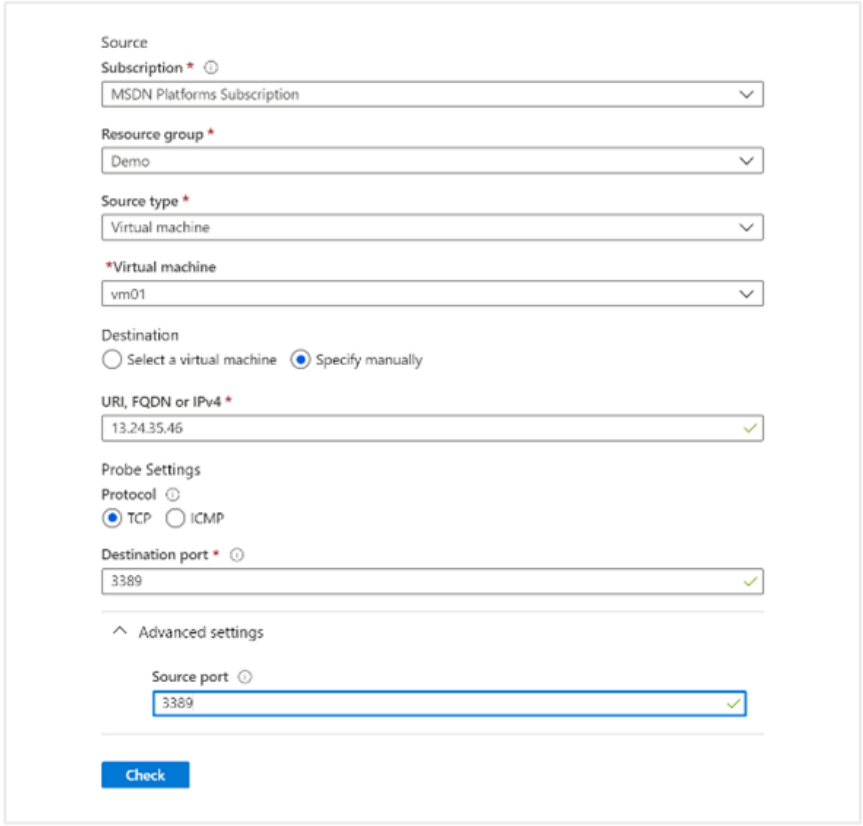
Check connectivity between source VM and destination

Identify configuration issues that are impacting reachability

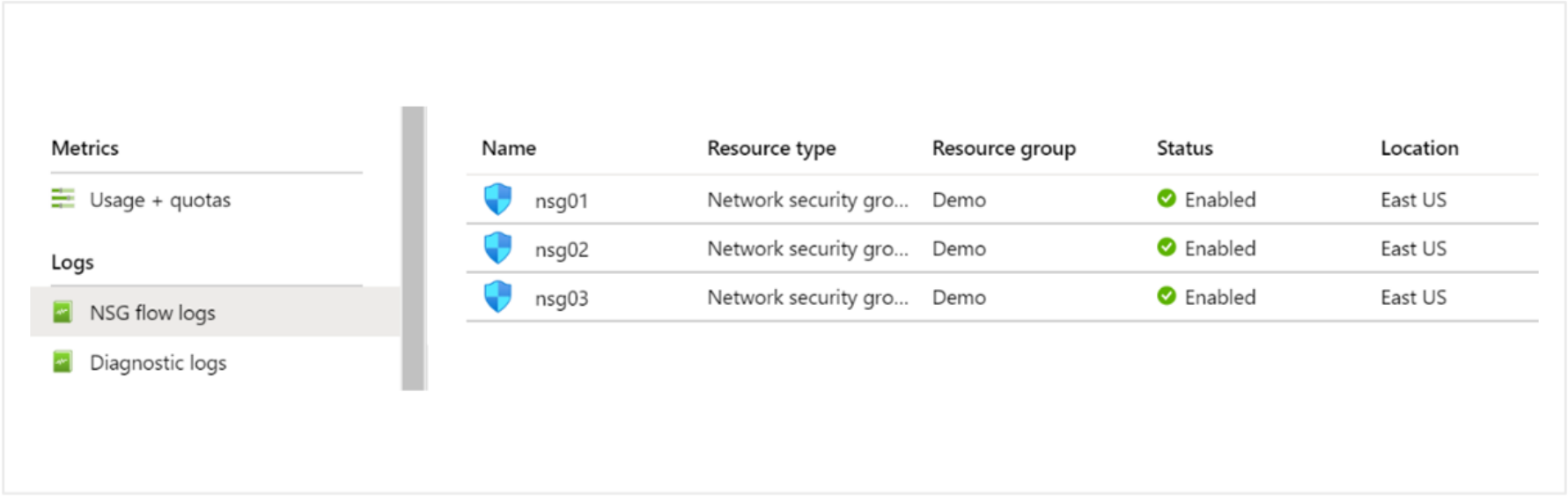
Provide all possible hop by hop paths from the source to destination

Review hop by hop latency – min, max, and average between source and destination

View a graphical topology from your source to destination



Logs – NSG Flow Logs

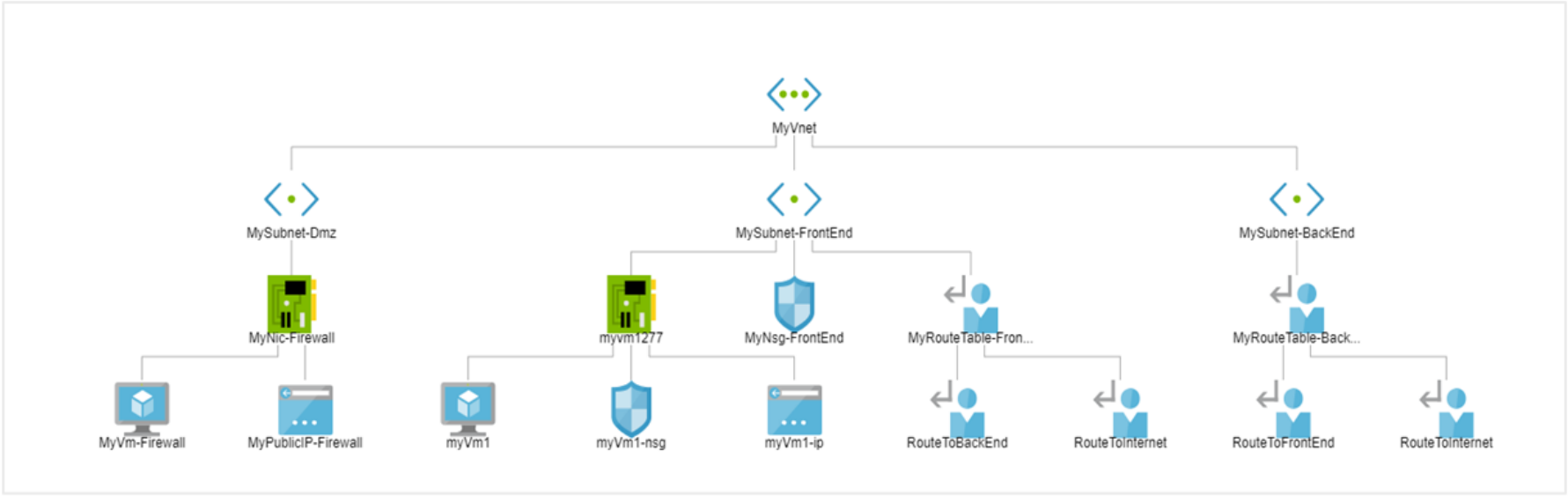


View information about ingress and egress IP traffic through an NSG

Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis

The JSON format can be visually displayed in Power BI or third-party tools like Kibana

Monitoring – Topology



Provides a visual representation of your networking elements

View all the resources in a virtual network, resource to resource associations, and relationships between the resources

The Network Watcher instance in the same region as the virtual network

Final Summary – 2 Days Azure Webinar


Module 01: Identity


Module 02: Governance and Compliance


Module 03: Azure Administration


Module 04: Virtual Networking


Module 05: Intersite Connectivity

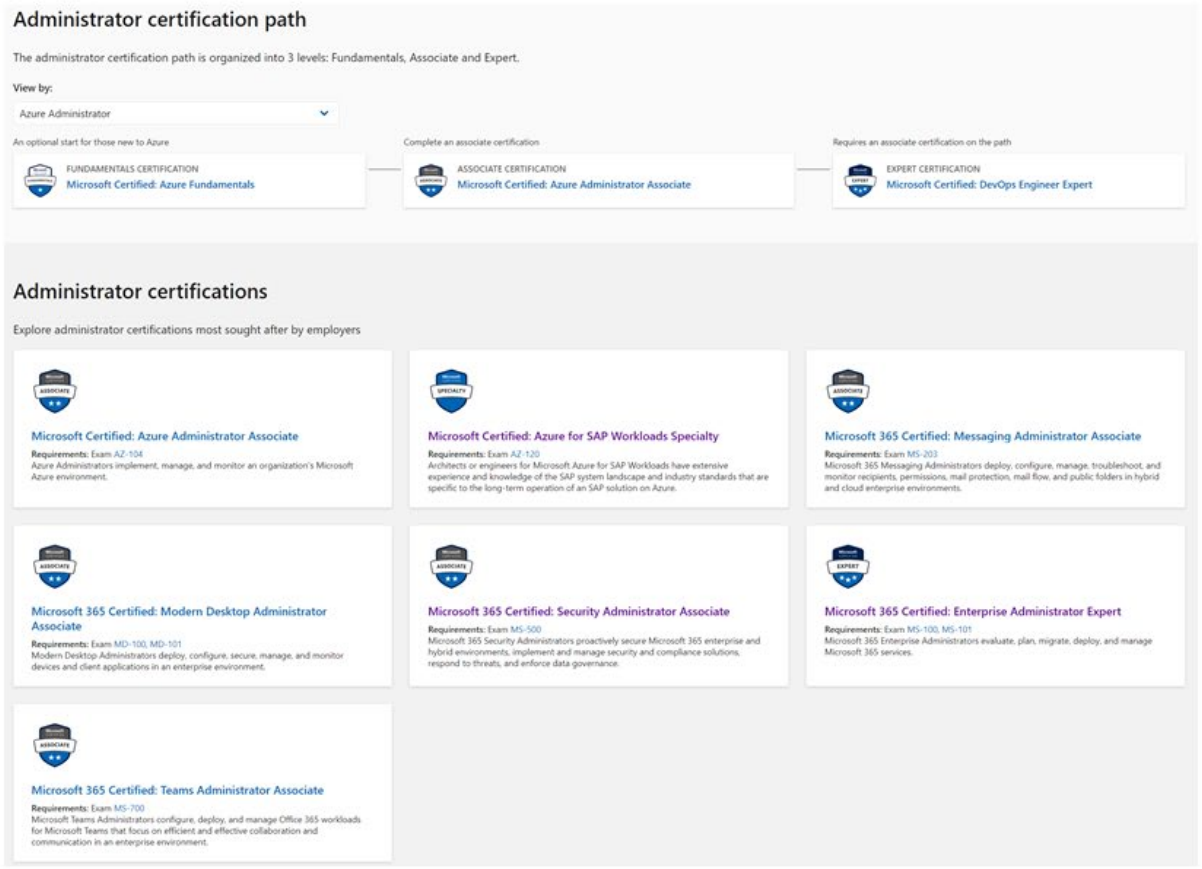

Module 06: Network Traffic Management


Module 07: Azure Storage


Module 08: Azure Virtual Machines


Module 09: Monitoring

Final Summary – 2 Days Azure Webinar



End of presentation

Thanks for your attention