



AZ-104T00A

Module 01:

Identity



Module Overview

- Azure Active Directory (now Microsoft Entra ID)
- Users and Groups

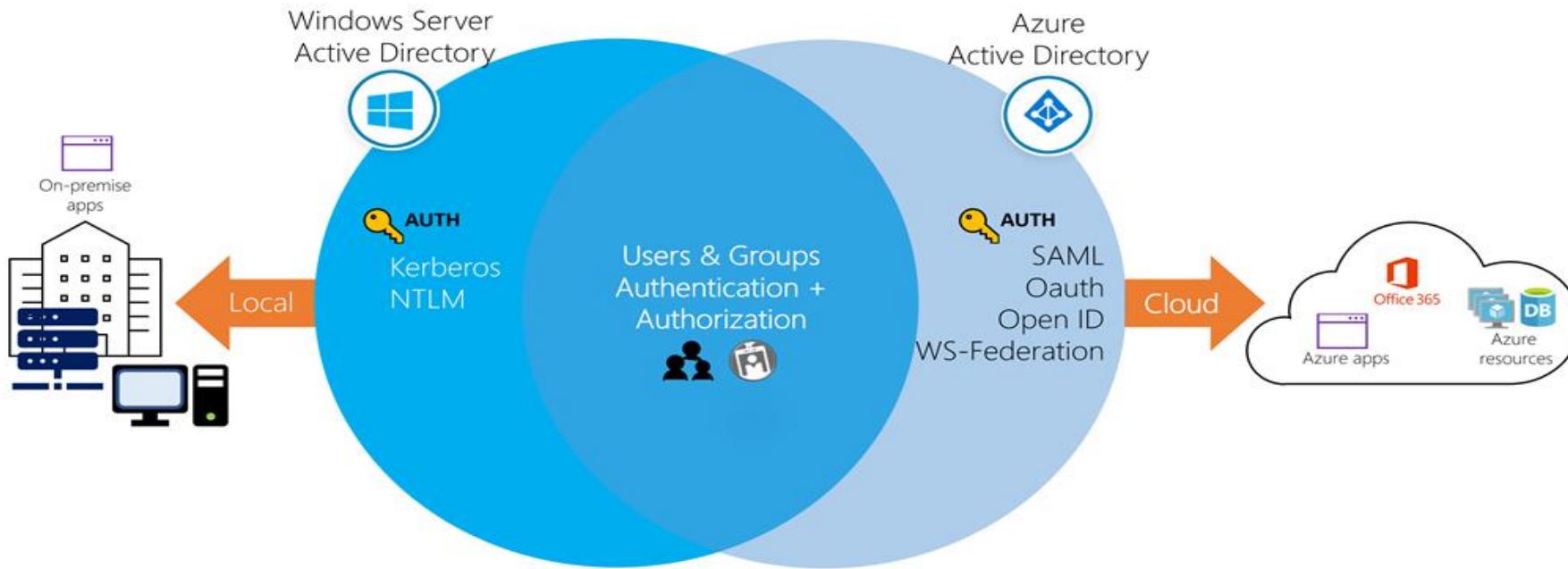
Azure Active Directory



Azure Active Directory Overview

- Azure Active Directory
- Azure AD Concepts
- AD DS vs. Azure Active Directory
- Azure Active Directory Editions
- Azure AD Join
- Multi-Factor Authentication
- 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 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.
User subscription	Used to pay for Azure cloud services.

AD DS vs Azure Active Directory

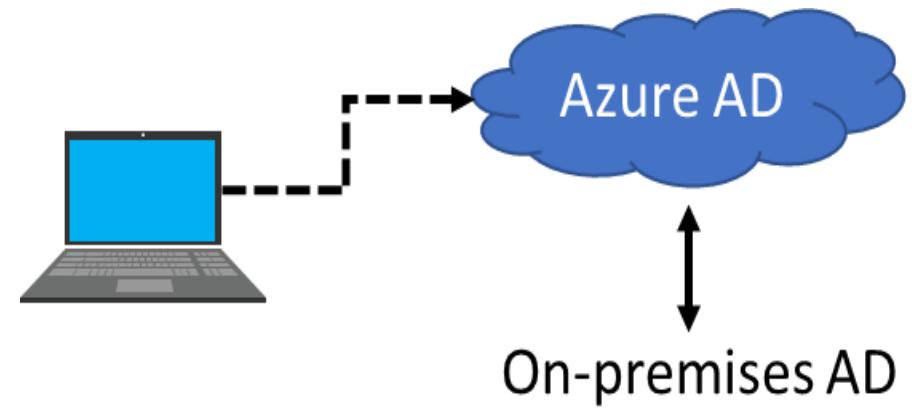
- Azure AD is primarily an identity solution, and designed for HTTP and HTTPS communications
- Queried using the REST API over HTTP and HTTPS. Instead of LDAP.
- Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization). Instead of 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

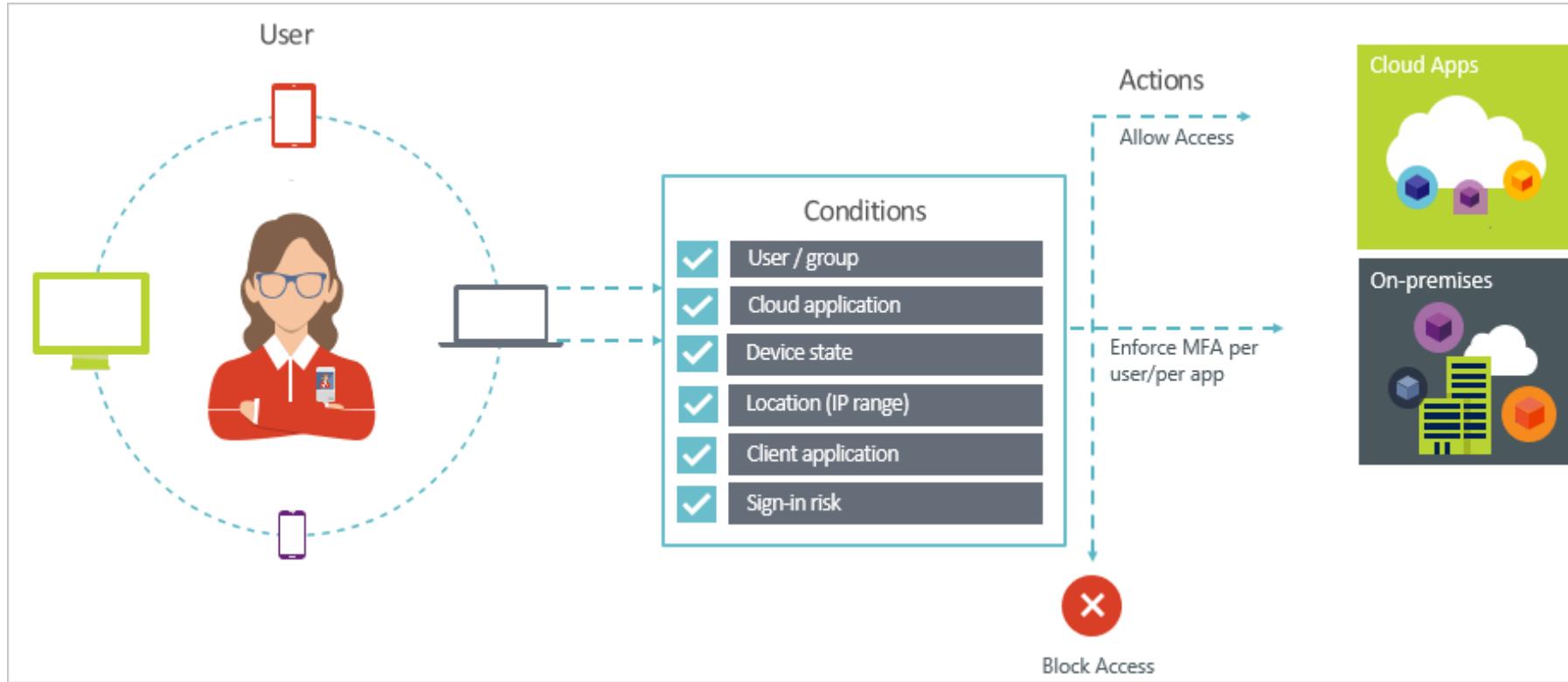
Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features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



Multi-Factor Authentication



Conditions – “When this happens”
Access controls – “Then do this”

- Provides two step authentication verification
- Lets you enforce controls on access to apps based on specific conditions

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)

Password reset - Authentication methods
mitaric (Default Directory) - Azure Active Directory

Save Discard

Number of methods required to reset

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Number of questions required to register

Number of questions required to reset

Select security questions
5 security questions selected

The screenshot shows the 'Password reset - Authentication methods' configuration page in the Azure Active Directory portal. It includes sections for 'Manage' (Properties, Authentication methods, Registration), 'Activity' (Audit logs, Usage & insights), and 'Troubleshooting + Support' (New support request). The 'Authentication methods' section is highlighted with yellow circles numbered 1, 2, and 3, corresponding to the steps in the list above. The 'Number of methods required to reset' is set to 1. The 'Methods available to users' section lists Email, Mobile phone, and Security questions as checked options. The 'Number of questions required to register' is set to 5, and the 'Number of questions required to reset' is also set to 5. A note at the bottom indicates 5 security questions have been selected.

Users and Groups



Users and Groups Overview

- User Accounts
- Managing User Accounts
- Bulk User Accounts
- Group Accounts
- Azure AD Connect

User Accounts

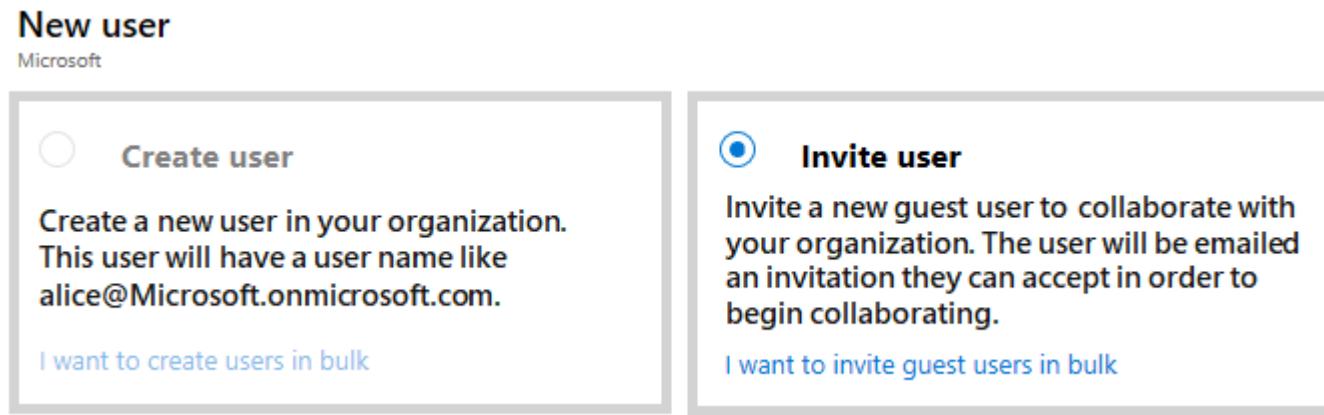
The screenshot shows the 'Users | All users' page in Microsoft Azure Active Directory. The left sidebar includes links for 'All users', 'Deleted users', 'Password reset', 'User settings', and 'Diagnose and solve problems'. The main area displays a table with the following data:

Name	User name	User type	Source
Ziaulla	ziaulla@mac...	Guest	External Azure Active Directory
Retail Crisis Notificati	rscrisis@mic...	Member	Windows Server AD
"Planning & Launch Se	plsoem@mi...		Windows Server AD
'amckenziec	'amckenziec...	Guest	Invited user
'Evento FY20 Colombia	kickcolo@mi...	Member	Windows Server AD

- All users must have an account
- The account is used for authentication and authorization
- Identity Sources: Cloud, Directory-synchronized, and Guest

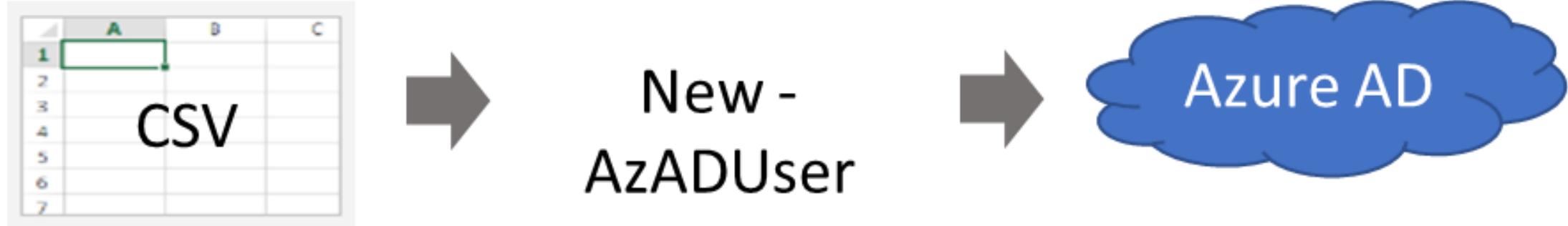
Managing User Accounts

[+ New user](#) [+ New guest user](#) [↑ Bulk create](#) [↑ Bulk invite](#) [↑ Bulk delete](#) [↓ Download users](#) [⟳ Refresh](#) [🔑 Reset password](#) [🔗 Multi-Factor Authentication](#) [...](#)



- 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)

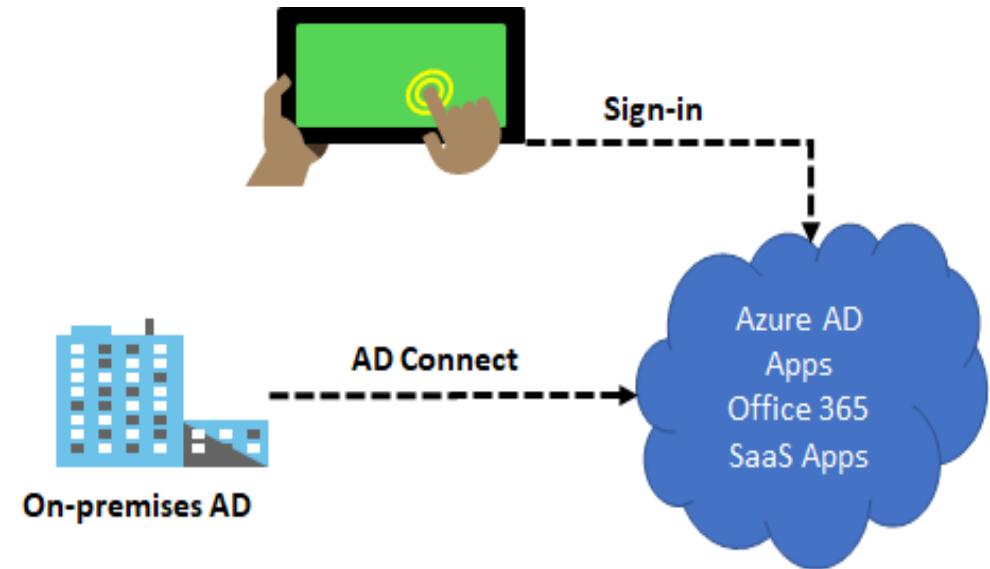


A screenshot of a web-based application interface for managing group accounts. At the top, there is a search bar labeled "Search groups" with a magnifying glass icon and a button labeled "Add filters" with a plus sign and filter icon. Below the search bar is a table with four columns: "Name", "Group Type", and "Membership Type". The "Name" column contains three entries: "Managers", "Virtual Machine Administrators", and "Virtual Network Administrators", each preceded by a small checkbox. To the right of the "Name" column are the "Group Type" and "Membership Type" columns, both of which show "Security" and "Assigned" respectively for all three groups.

Name	Group Type	Membership Type
<input type="checkbox"/> MA Managers	Security	Assigned
<input type="checkbox"/> VM Virtual Machine Administrators	Security	Assigned
<input type="checkbox"/> VN Virtual Network Administrators	Security	Assigned

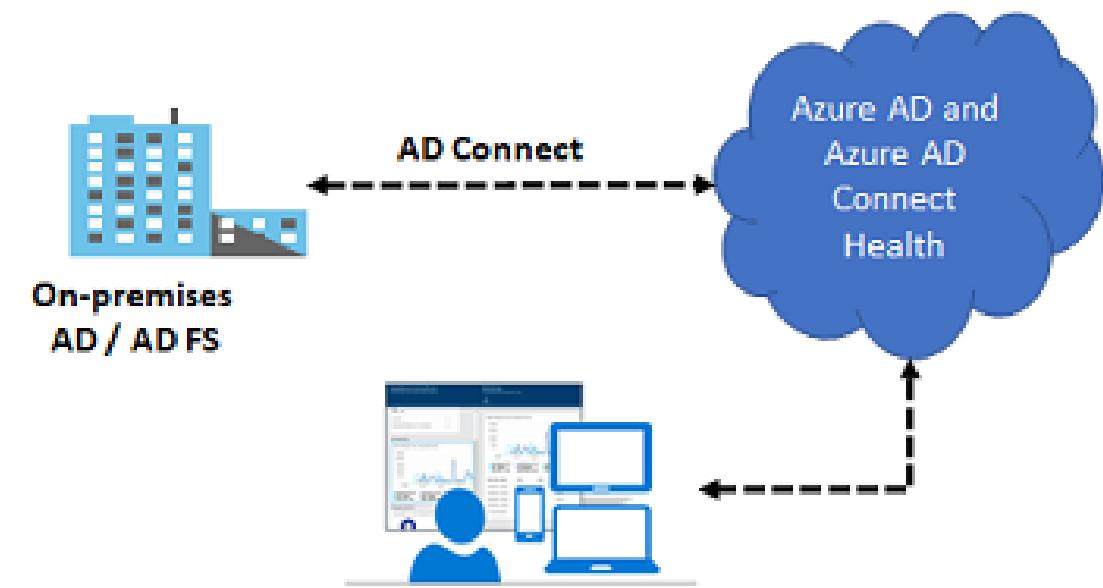
Azure AD Connect

- Integrate your on-premises directories with Azure Active Directory
- Provides a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD
- There are several authentication options – password hash synchronization and pass-through authentication



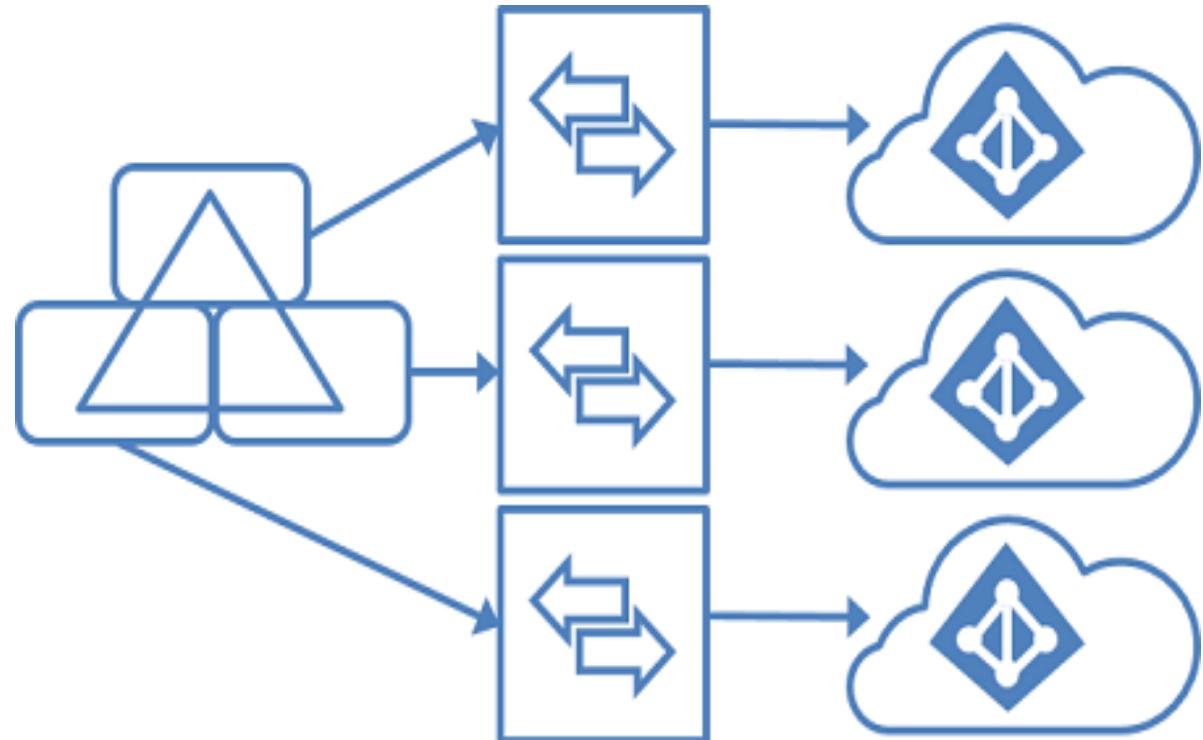
Azure AD Connect Health

- Monitor and gain insights into AD FS servers, Azure AD Connect, and AD domain controllers
- Monitor and gain insights into the synchronizations that occur between your on-premises AD DS and Azure AD
- Monitor and gain insights into your on-premises identity infrastructure that is used to access Office 365 or other Azure AD applications



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

Module 01 Lab and Review



AZ-104T00A

Module 02:

Governance and Compliance



Module Overview

- Subscriptions and Accounts
- Azure Policy
- Role-based Access Control

Subscriptions and Accounts



Subscriptions and Accounts Overview

- Regions
- Azure Subscriptions
- Getting a Subscription
- Subscription Usage
- Cost Management
- Resource Tags
- Cost Savings

Regions

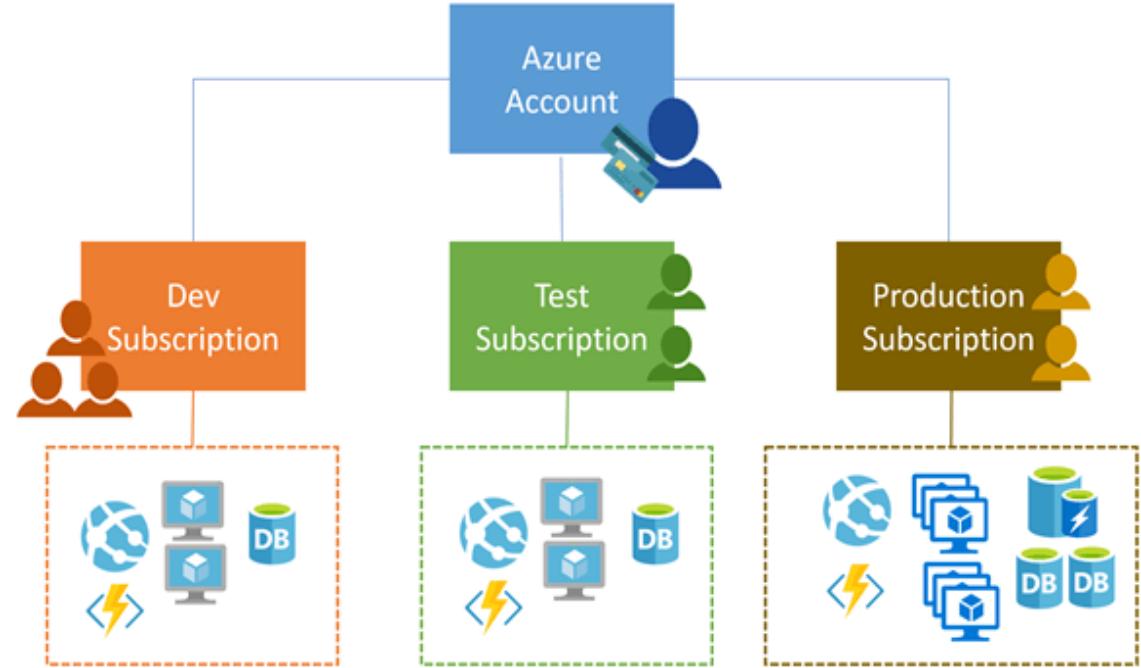
- A region represents a collection of datacenters
- Provides flexibility and scale
- Preserves data residency
- Select regions close to your users
- Be aware of region deployment availability
- There are global services that are region independent
- Regions are paired for high availability



Worldwide there are 50+ 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

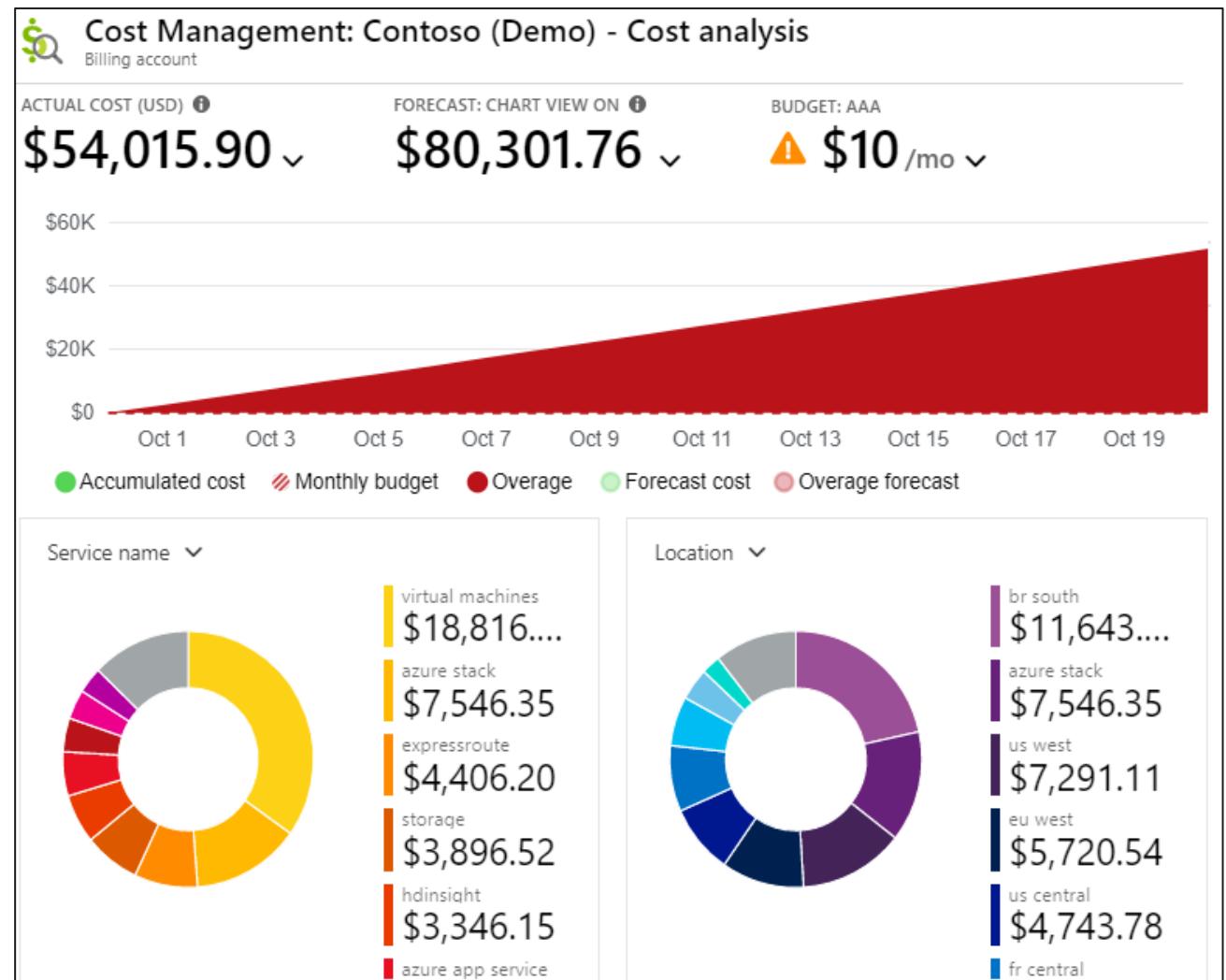


Subscription Usage

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

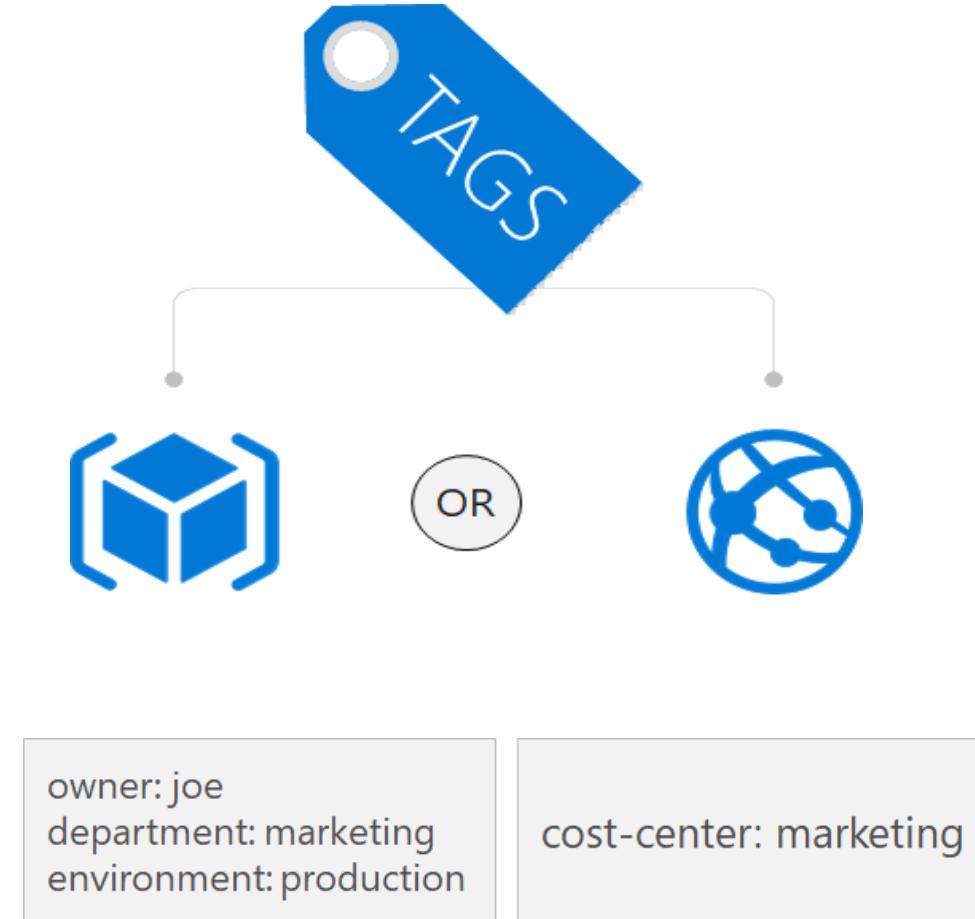
Cost Management

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



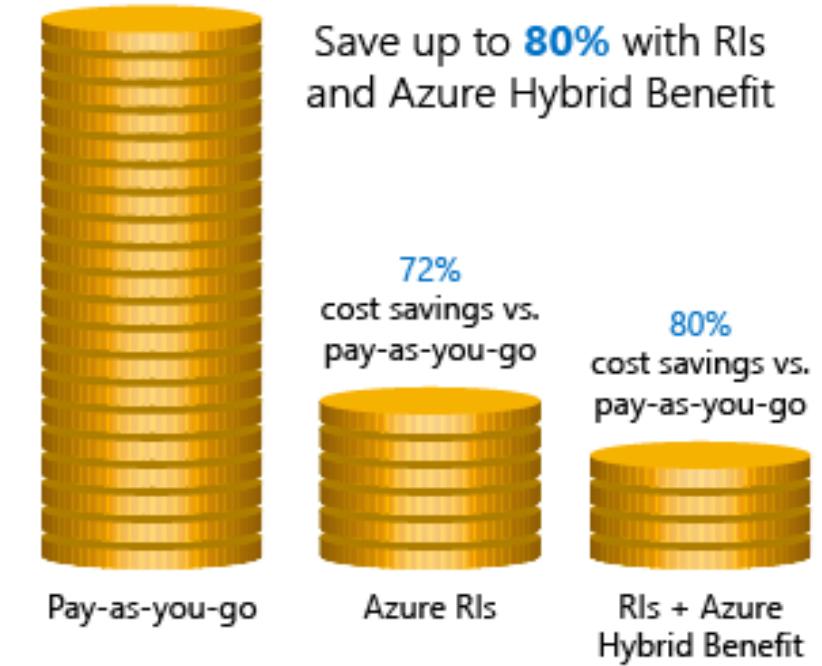
Resource Tags

- 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



Azure Policy

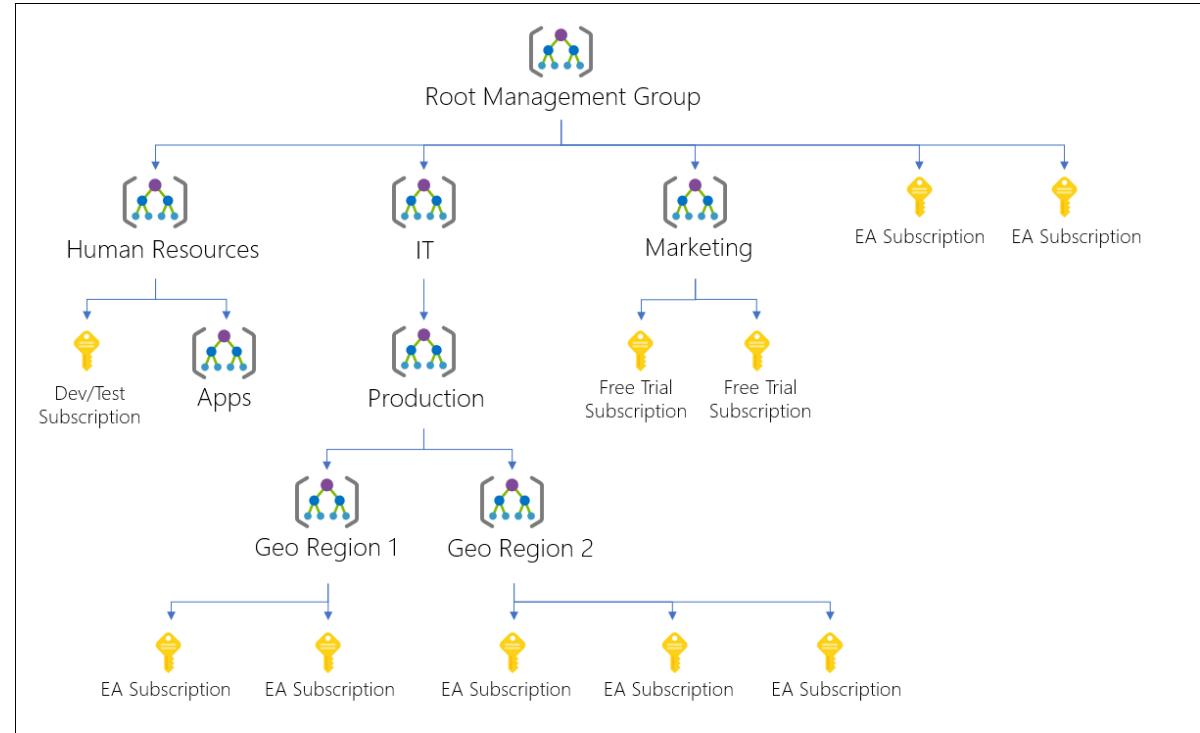


Azure Policy Overview

- Management Groups
- Azure Policy
- Implementing Azure Policy
- Policy Definitions
- Create Initiative Definitions
- Scope the Initiative Definition
- Determine Compliance
- Demonstration – Azure Policy

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.

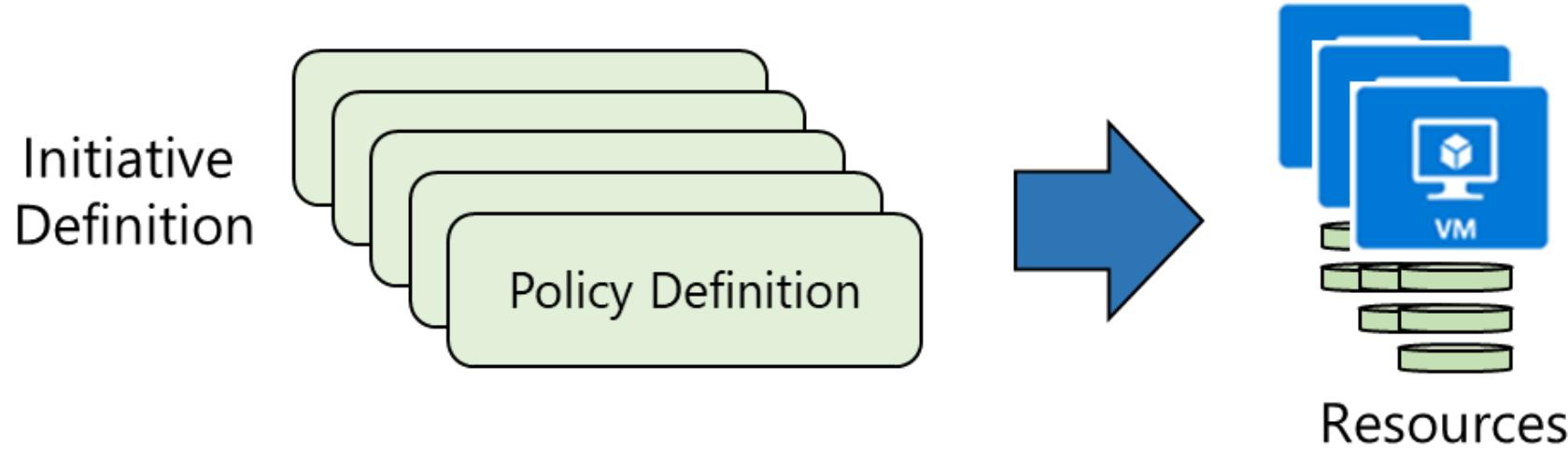
Allowed virtual machine SKUs – Specify a set of virtual machine SKUs that your organization can deploy.

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

Policy definition
New Policy definition

BASICS

Definition location *
Visual Studio Enterprise

Name * ⓘ
Github Sample Policy

Description
A sample policy from Github.

Category ⓘ
 Create new Use existing
Category

POLICY RULE

↓ Import sample policy definition from GitHub

Create Initiative Definitions

- Group policy definitions
- Include one or more policies
- Requires planning

Initiative definition
New Initiative definition

BASICS

Definition location *

Visual Studio Enterprise ...

Name * ⓘ

East Region ✓

Description ⓘ

East Region Initiative Definition

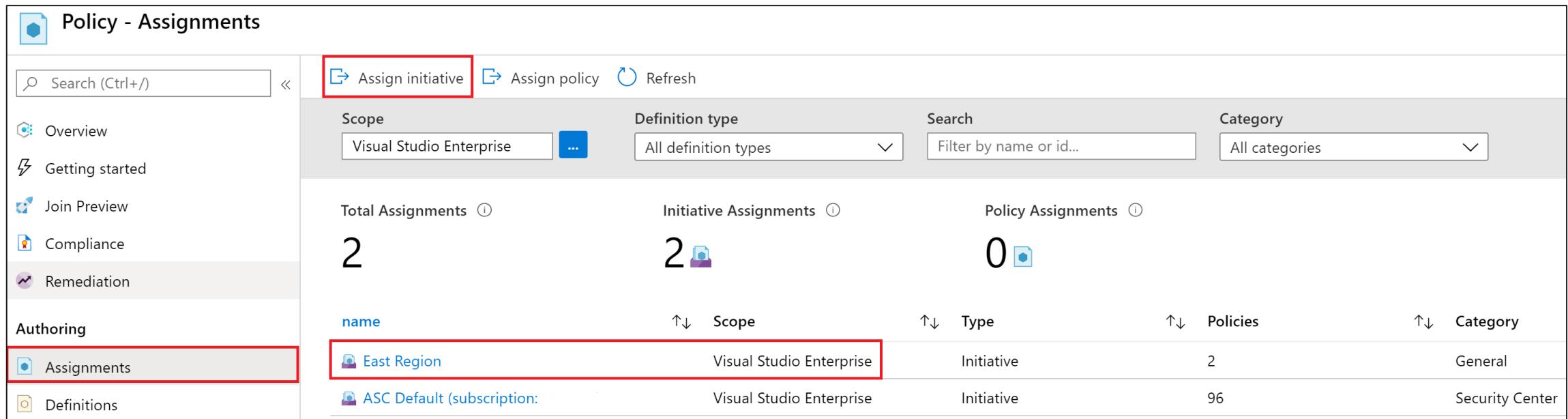
Category ⓘ

Create new Use existing

General ▼

namingPolicyDefinition	Policy to specify allowed naming convention	Custom	Delete
regionPolicyDefinition	Policy to allow resource creation only in certain regions	Custom	Delete

Scope the Initiative Definition



The screenshot shows the 'Policy - Assignments' blade in the Azure portal. The left sidebar includes links for Overview, Getting started, Join Preview, Compliance, Remediation, Authoring (with 'Assignments' selected), and Definitions. The main area has sections for Total Assignments (2), Initiative Assignments (2), and Policy Assignments (0). Below these are two rows of data:

name	Scope	Type	Policies	Category
East Region	Visual Studio Enterprise	Initiative	2	General
ASC Default (subscription)	Visual Studio Enterprise	Initiative	96	Security Center

- Assign the definition to a scope
- The scope enforces the policy
- Select the subscription, and optionally the resource group

Determine Compliance

Policy - Compliance

Search (Ctrl+ /) Assign policy Assign initiative Refresh

Overview Getting started Join Preview **Compliance** Remediation

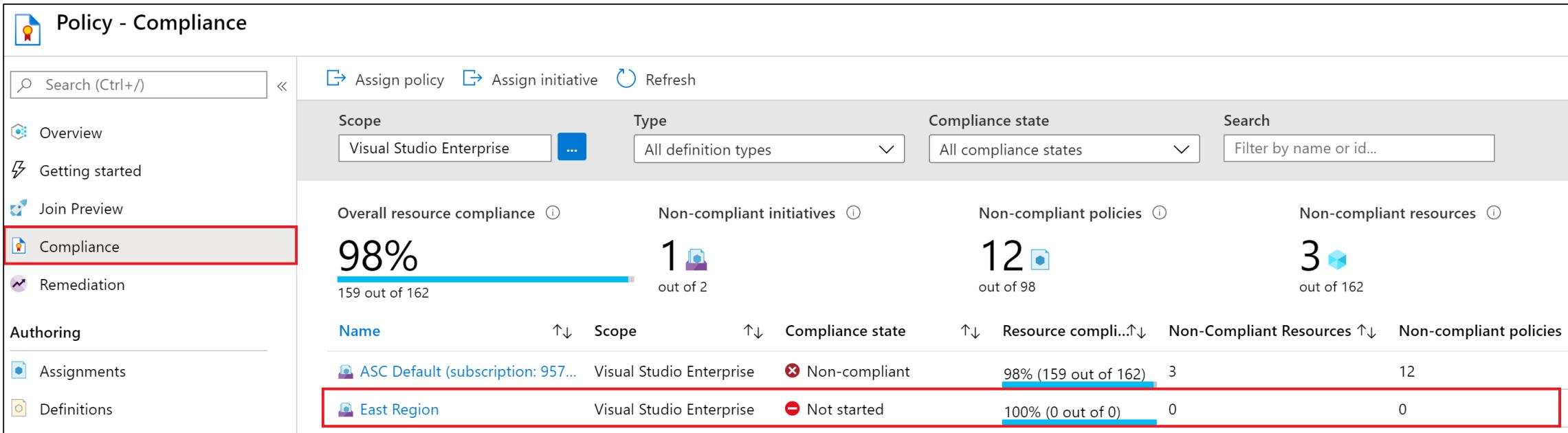
Scope Type Compliance state Search

Visual Studio Enterprise All definition types All compliance states Filter by name or id...

Overall resource compliance (98%) Non-compliant initiatives (1) Non-compliant policies (12) Non-compliant resources (3)

159 out of 162 out of 2 out of 98 out of 162

Name	Scope	Compliance state	Resource compli...	Non-Compliant Resources	Non-compliant policies
ASC Default (subscription: 957...)	Visual Studio Enterprise	Non-compliant	98% (159 out of 162)	3	12
East Region	Visual Studio Enterprise	Not started	100% (0 out of 0)	0	0



- Non-compliant initiatives
- Non-compliant policies
- Non-compliant resources

Role-Based Access Control



Role-Based Access Control Overview

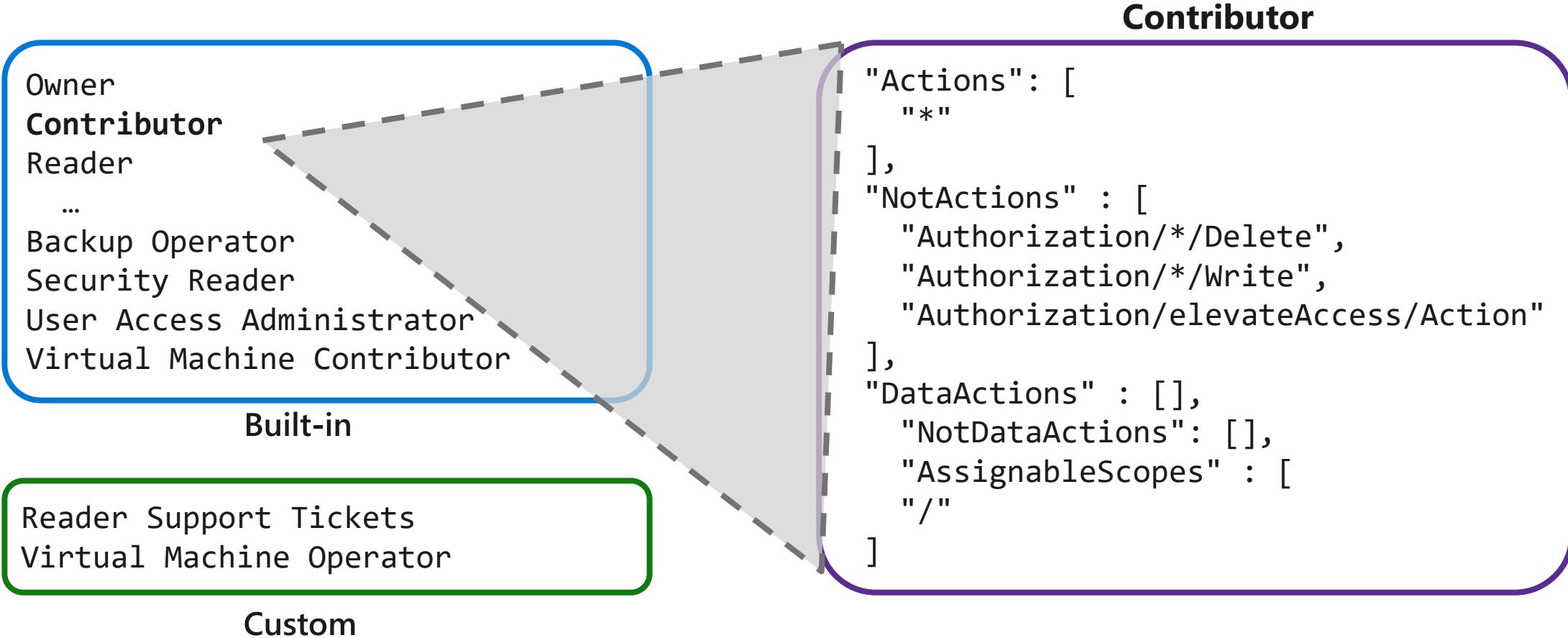
- Role-Based Access Control
- Role Definition
- Role Assignment
- Azure RBAC Roles vs Azure AD Administrator Roles
- RBAC Authentication
- Azure RBAC Roles

Role-Based Access Control

- Provides fine-grained access management of resources in Azure
 - 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
- Concepts
 - **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

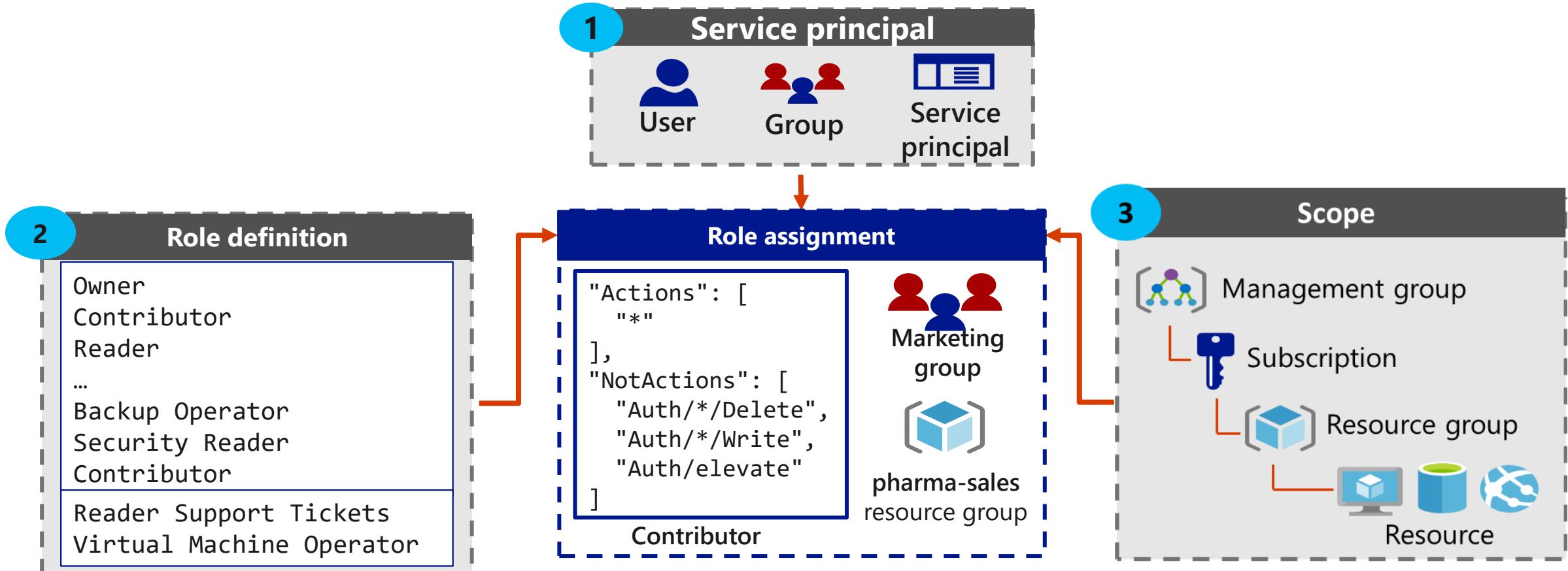
Role Definition

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



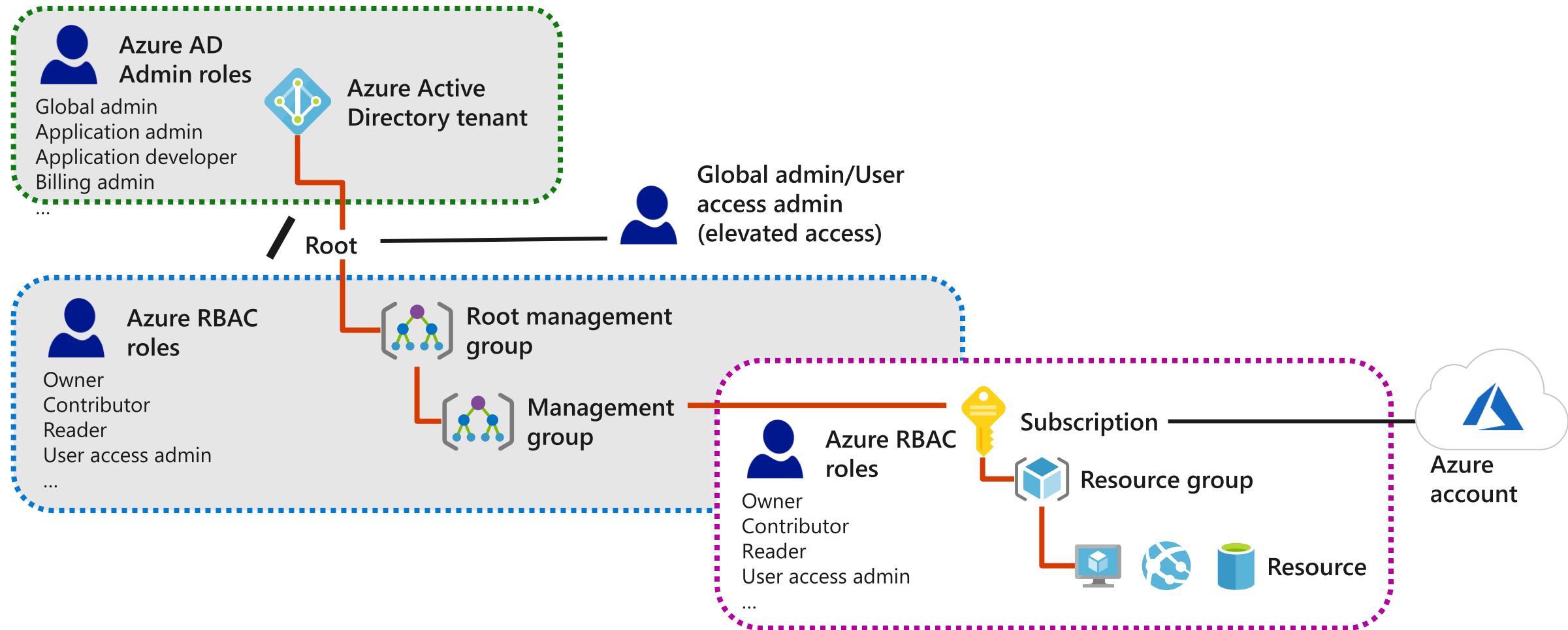
Azure RBAC Roles vs. Azure AD Roles

Azure and Azure AD offer two types of RBAC 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.

Module 02 Lab and Review





AZ-104T00A

Module 03:

Azure Administration



Module Overview

- Resource Manager
- Azure Portal and Cloud Shell
- Azure PowerShell and CLI
- ARM Templates

Resource Manager

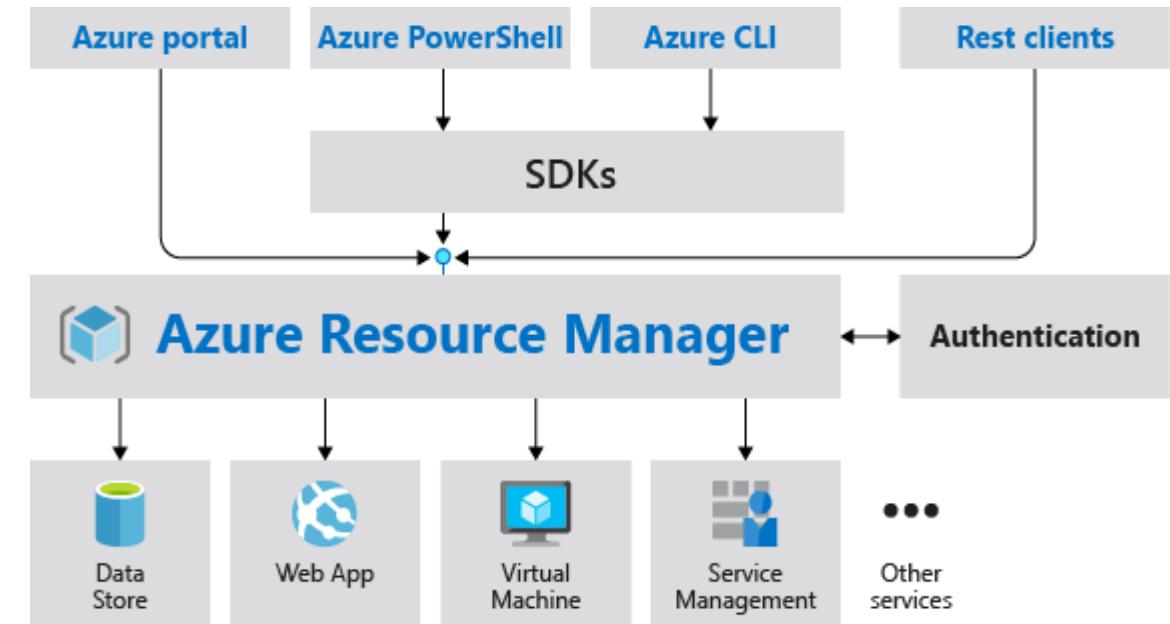


Resource Manager Overview

- 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

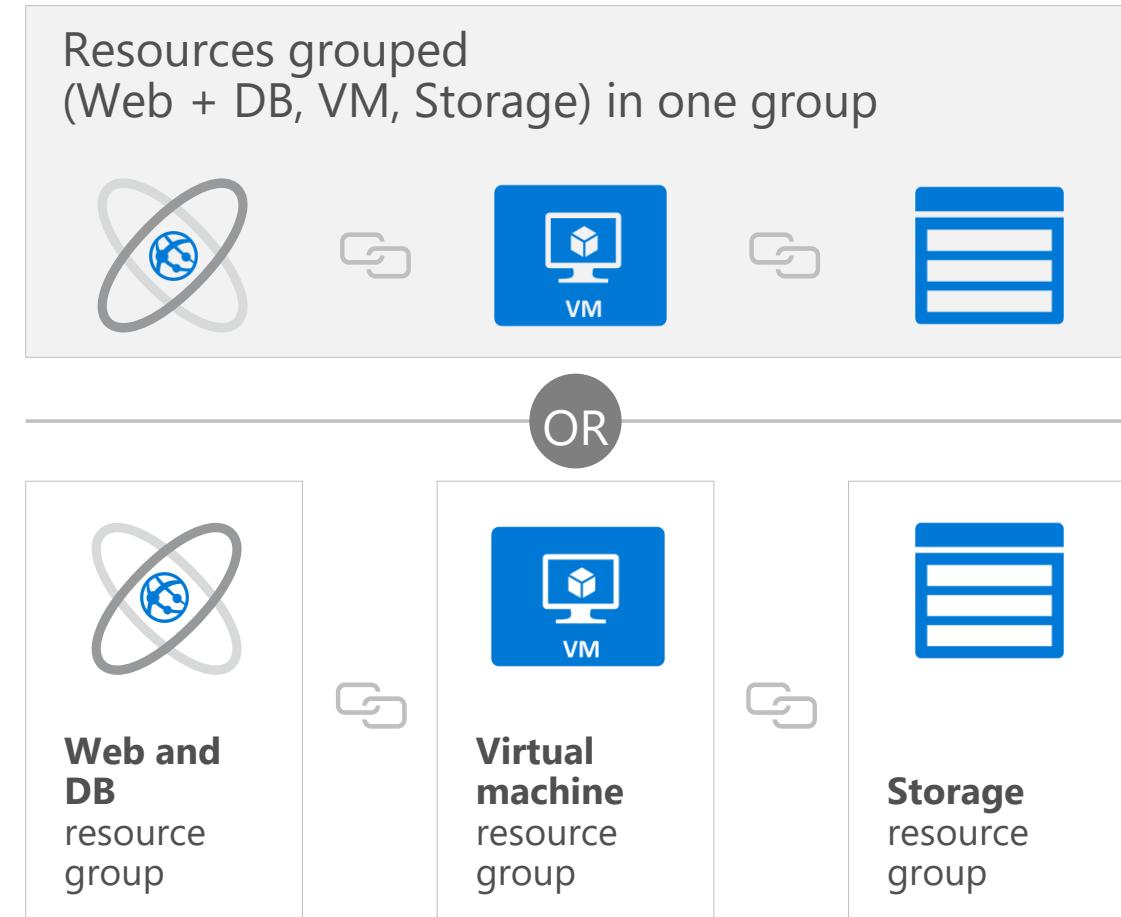


Terminology

- 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

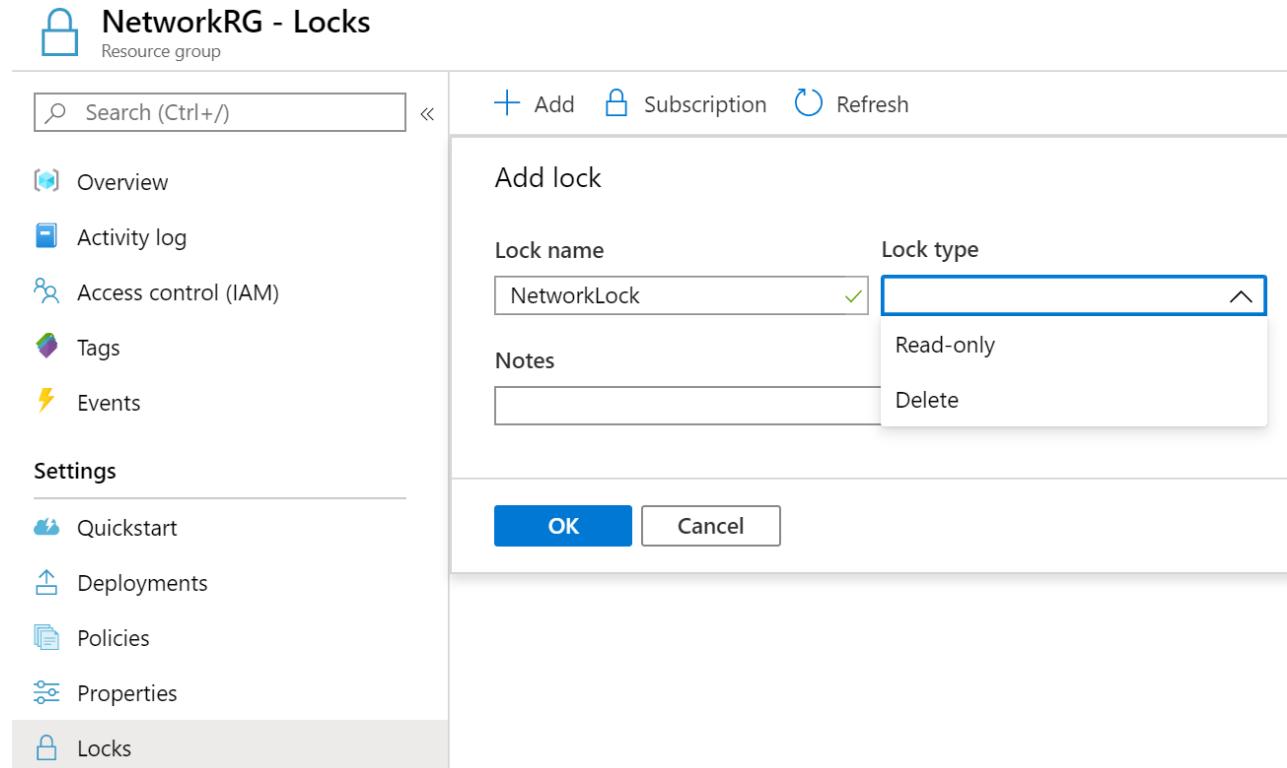
- Resources can only exist in one resource group
- Groups cannot be renamed
- Groups can have resources of many different types (services)
- Groups can have resources from many different regions
- Deployments are incremental



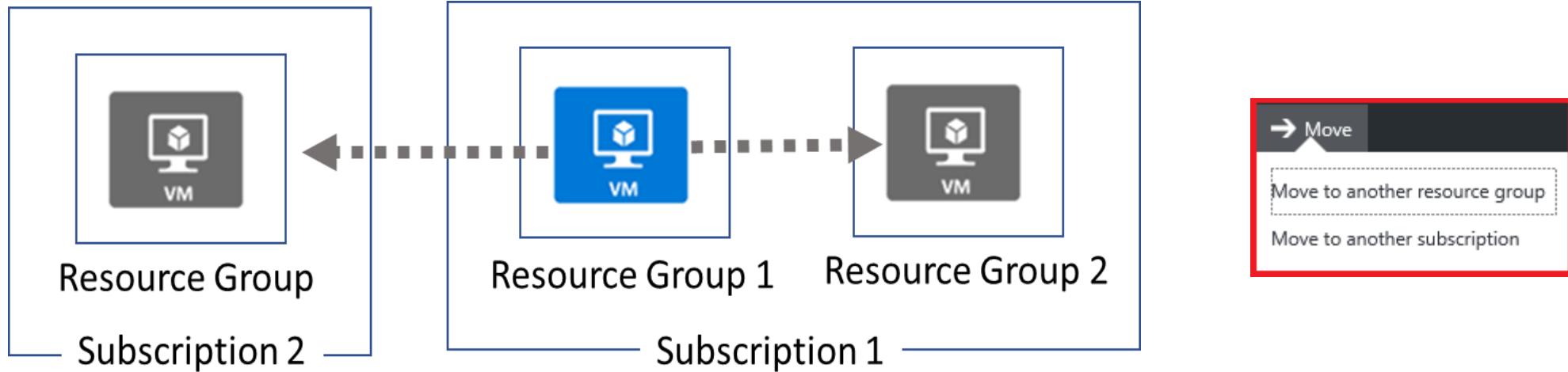
✓ By scoping permissions to a resource group, you can add/remove and modify resources easily

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



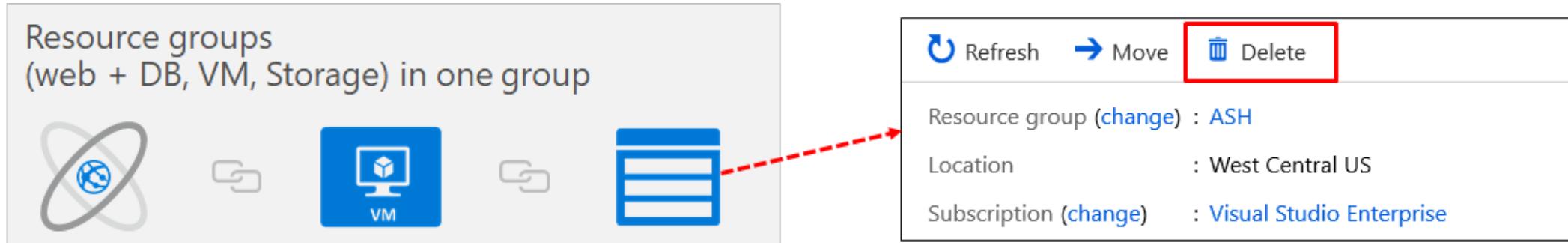
Moving Resources



- When moving resources, both the source group and the target group are locked during the operation
- Services that cannot be moved: AD Domain Services, ExpressRoute, and Site Recovery. Other restrictions apply.

Removing Resources and Resource Groups

- Remove Azure resources that you no longer use
- Ensures you will not see unexpected charges
- Remove individual resources or remove the resource group



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

Resource Limits

ASC DEMO | Usage + quotas

Subscription

Settings

Programmatic deployment

Resource groups

Resources

Usage + quotas

Policies

Security

Events

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. [Learn more](#)

[Request Increase](#)

Quota	Provider	Location	Usage	
Total Regional vCPUs	Microsoft.Compute	East US	<div style="width: 25%; background-color: #2e7131;"></div>	25 % 25 of 100
Total Regional vCPUs	Microsoft.Compute	West Europe	<div style="width: 21%; background-color: #2e7131;"></div>	21 % 21 of 100
Total Regional vCPUs	Microsoft.Compute	Central US	<div style="width: 17%; background-color: #2e7131;"></div>	17 % 17 of 100
Standard Dv2 Family vCPUs	Microsoft.Compute	West Europe	<div style="width: 16%; background-color: #2e7131;"></div>	16 % 16 of 100
Standard DSv2 Family vCPUs	Microsoft.Compute	Central US	<div style="width: 14%; background-color: #2e7131;"></div>	14 % 14 of 100

- 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

Azure Portal and Cloud Shell

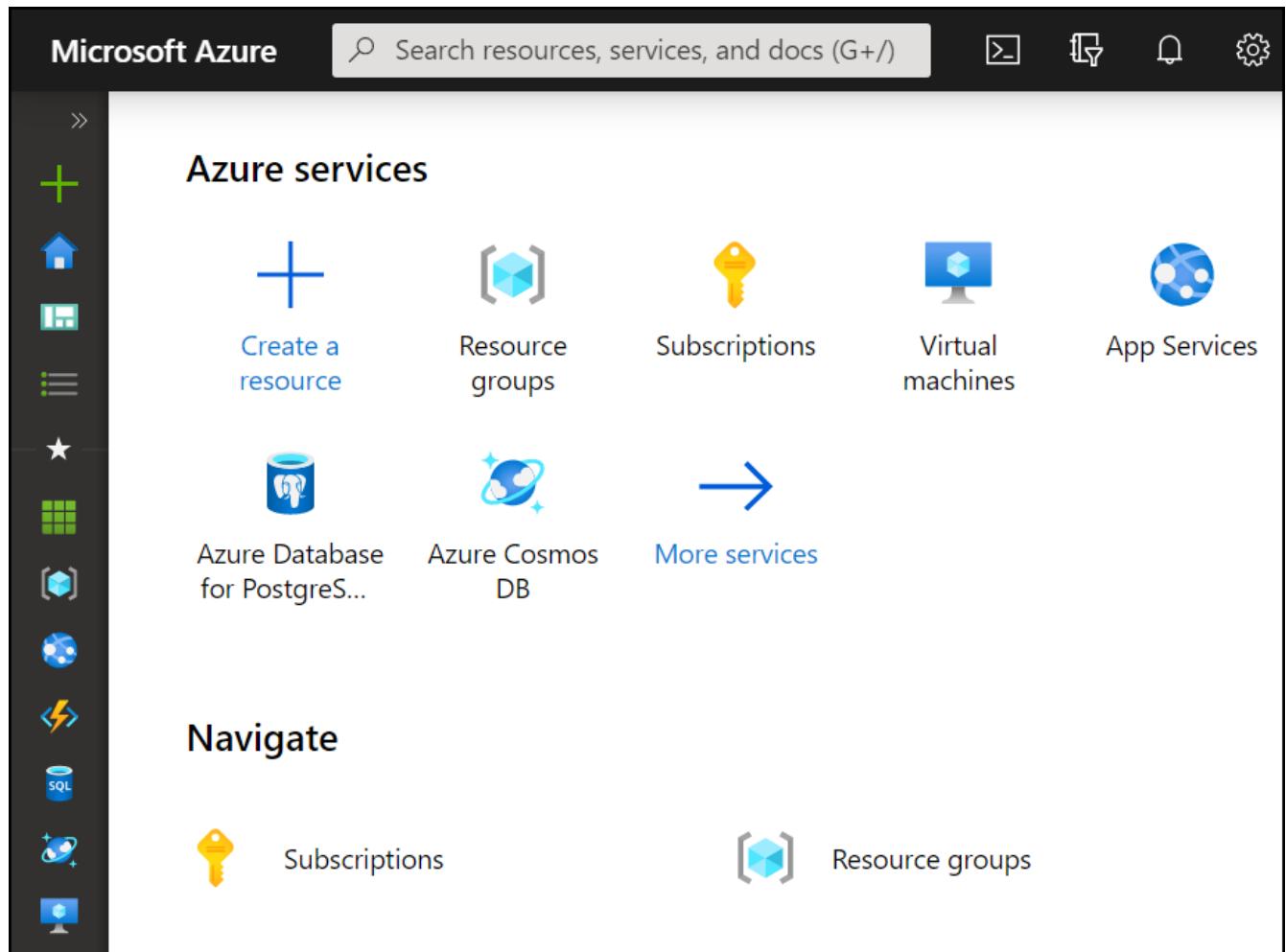


Azure Portal and Cloud Shell Overview

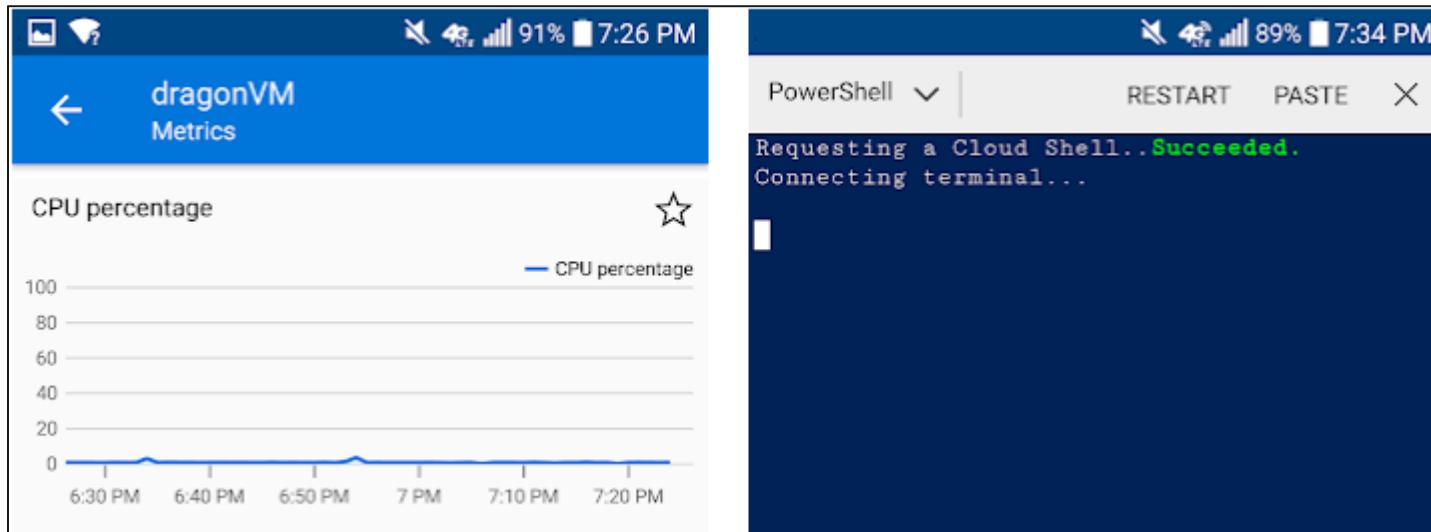
- Azure Portal
- Azure Mobile App
- Demonstration – Azure Portal
- Azure Cloud Shell
- Demonstration – Cloud Shell

Azure Portal

- Search resources, services, and docs
- Manage resources
- Create customized dashboards and favorites
- Access the Cloud Shell
- Receive notifications



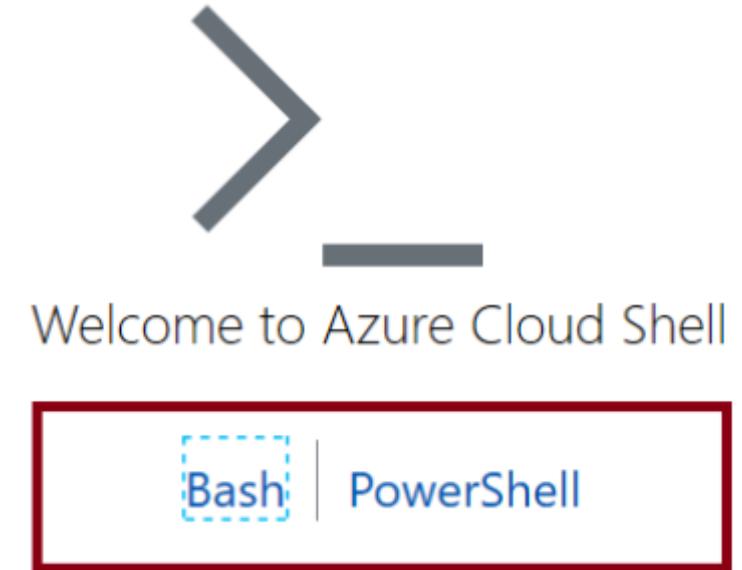
Azure Mobile App



- Stay connected to the cloud
- Check status and critical metrics anytime, anywhere
- Diagnose and fix issues quickly
- Run commands to manage your Azure resources

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



Azure PowerShell and CLI



Azure PowerShell and CLI Overview

- Azure PowerShell
- PowerShell Cmdlets and Modules
- Demonstration – Working with PowerShell Locally
- Azure CLI
- Demonstration – Working with Azure CLI Locally

Azure PowerShell

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

- Lets you connect to your Azure subscription and manage resources
- Adds the Azure-specific commands – new Az module
- 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

ARM Templates

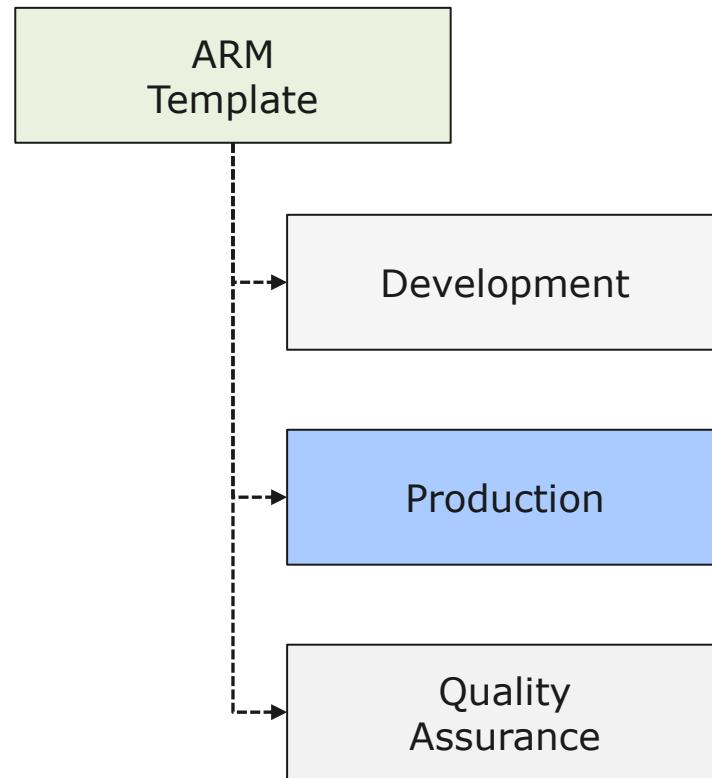


ARM Templates Overview

- Template Advantages
- Template Schema
- Template Parameters
- Template Variables
- Template Functions
- Template Resources
- Template Outputs
- 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."  
        }  
    }  
}
```

Template Variables

- Define values that are used throughout the template
- Makes your templates easier to maintain
- This example provides variables that describe networking features for a virtual machine

```
"variables": {  
    "nicName": "myVMNic",  
    "addressPrefix": "10.0.0.0/16",  
    "subnetName": "Subnet",  
    "subnetPrefix": "10.0.0.0/24",  
    "publicIPAddressName": "myPublicIP",  
    "virtualNetworkName": "MyVNET"  
}
```

Template Functions

- Reusable procedures
- Makes the template easier to maintain
- This function creates a unique name - use when creating resources that have globally unique naming requirements

```
"functions": [  
  {  
    "namespace": "contoso",  
    "members": {  
      "uniqueName": {  
        "parameters": [  
          {  
            "name": "namePrefix",  
            "type": "string"  
          } ],  
        "output": {  
          "type": "string",  
          "value":  
            "[concat(toLower(parameters('namePrefix')),  
            uniqueString(resourceGroup().id))]"  
        }      }    }  } ],
```

Template Resources

- Define the Azure resources that make up your deployment
- This example that creates a public IP address resource
- Name is a variable
- Location is a parameter

```
{  
  "type": "Microsoft.Network/publicIPAddresses",  
  "name": "[variables('publicIPAddressName')]",  
  "location": "[parameters('location')]",  
  "apiVersion": "2018-08-01",  
  "properties": {  
    "publicIPAllocationMethod": "Dynamic",  
    "dnsSettings": {  
      "domainNameLabel":  
        "[parameters('dnsLabelPrefix')]"  
    }  
  }  
}
```

Template Outputs

- Define any information you'd like to receive when the template runs
- This example receives a VM's IP address or FQDN
- Hostname is the output
- The FQDN value is read from the virtual machines public IP address settings

```
"outputs": {  
    "hostname": {  
        "type": "string",  
        "value": "[reference(variables(  
            'publicIPAddressName')).  
        dnsSettings.fqdn]"  
    }  
}
```

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

757 Quickstart templates are currently in the gallery.

[Create Configuration Manager Tech Preview Lab in Azure](#)

This template creates a new System Center Configuration Manager Technical Preview Lab environment. It creates 4 new Azure VMs, configuring a new AD Domain Contr...

 by [Yizhong Wu](#),
Last updated: 12/10/2018

[Create a Standard Storage Account](#)

This template creates a Standard Storage Account

 by [Brian Moore](#),
Last updated: 12/4/2018

[Deploy a Django app](#)

This template uses the Azure Linux CustomScript extension to deploy an application. This example creates an Ubuntu VM, does a silent install of Python, Django...

 by [Madhan Arumugam Ramakrishnan](#),
Last updated: 7/19/2018

[Create an new AD Domain with 2 Domain Controllers](#)

This template creates 2 new VMs to be AD DCs (primary and backup) for a new Forest and Domain

 by [Simon Davies](#),
Last updated: 7/5/2018

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

Module 03 Lab and Review





AZ-104T00A

Module 04:

Virtual Networking



Module Overview

- Virtual Networks
- IP Addressing
- Network Security Groups
- Azure Firewall
- Azure DNS

Virtual Networks

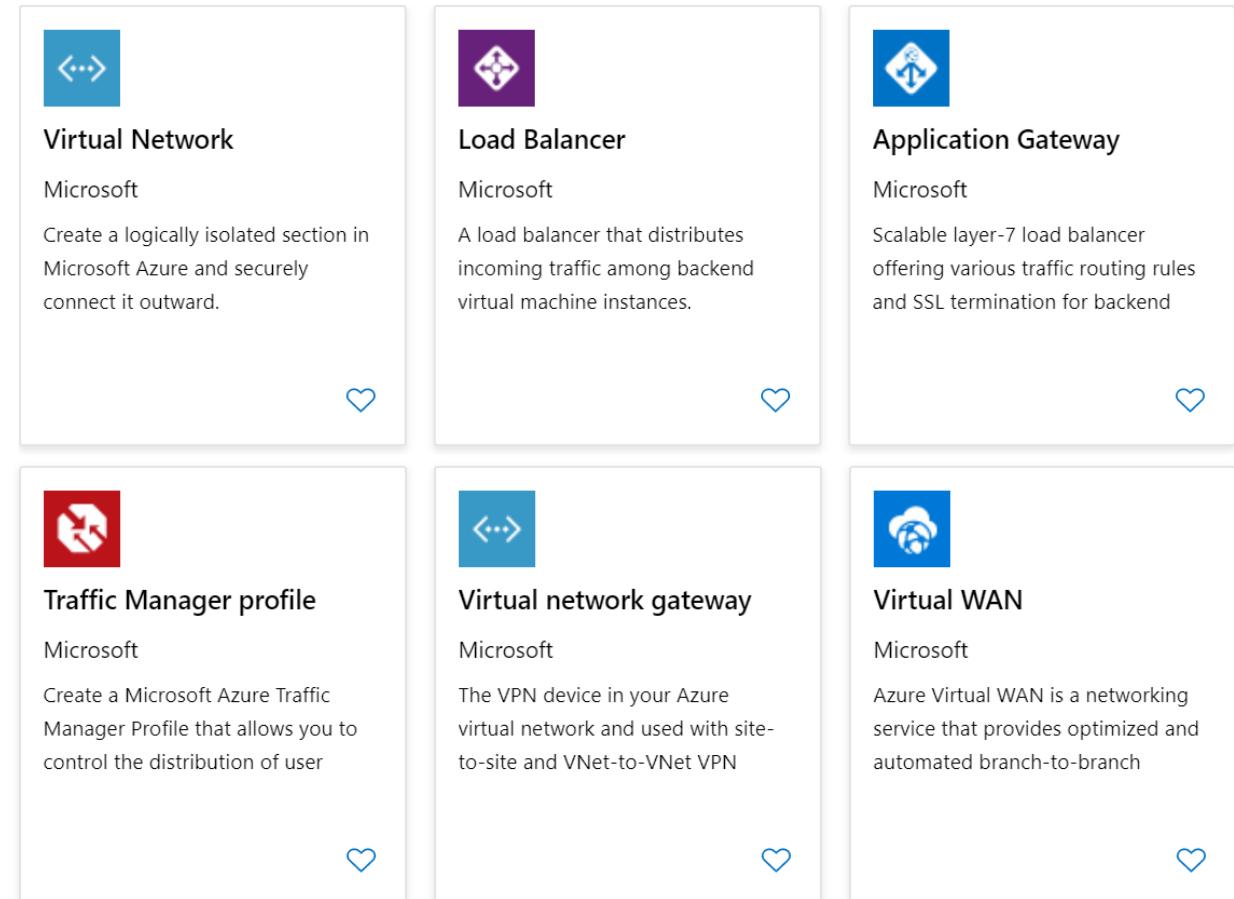


Virtual Networks Overview

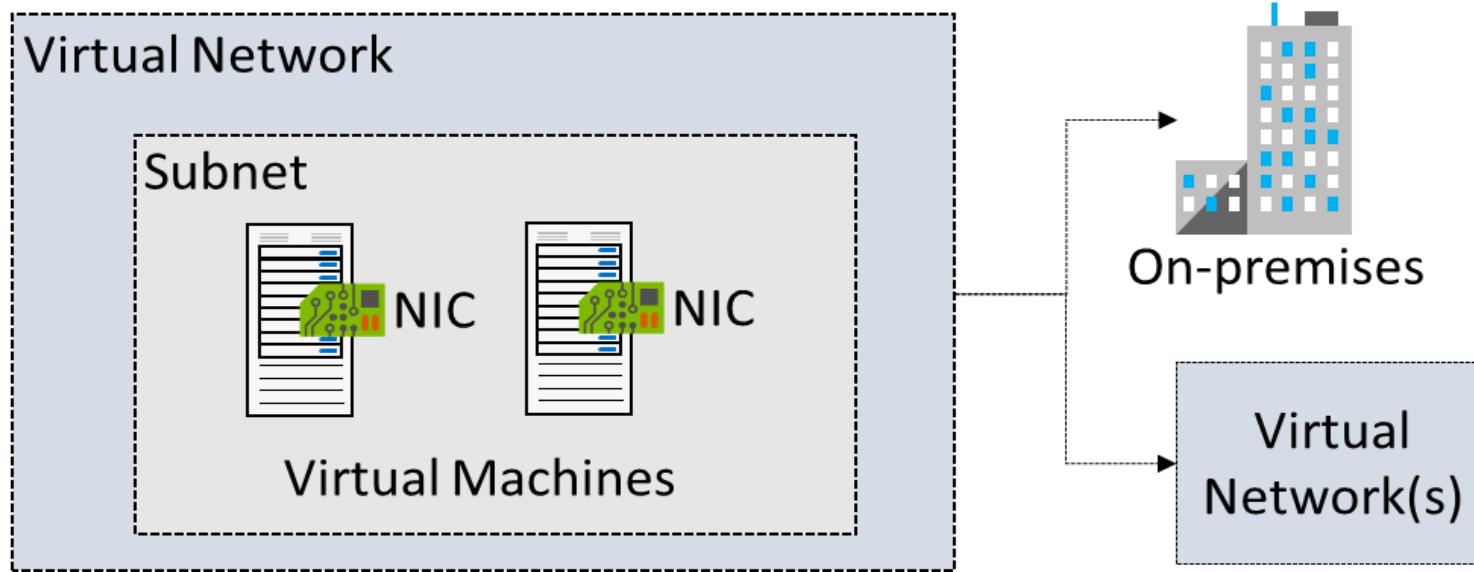
- Azure Networking Components
- Virtual Networks
- Subnets
- Implementing Virtual Networks

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

Subnets						
Actions		Subnet Details				
Name	Address range	IPv4 available addresses	Delegated to	Security group		
subnet0	10.1.0.0/24	251	-	nsg0		
subnet1	10.1.1.0/24	251	-	-		
subnet2	10.1.2.0/24	251	-	nsg2		
GatewaySubnet	10.1.255.0/24	251	-	-		

- 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

Create virtual network

Basics IP Addresses Security Tags Review + create

Project details

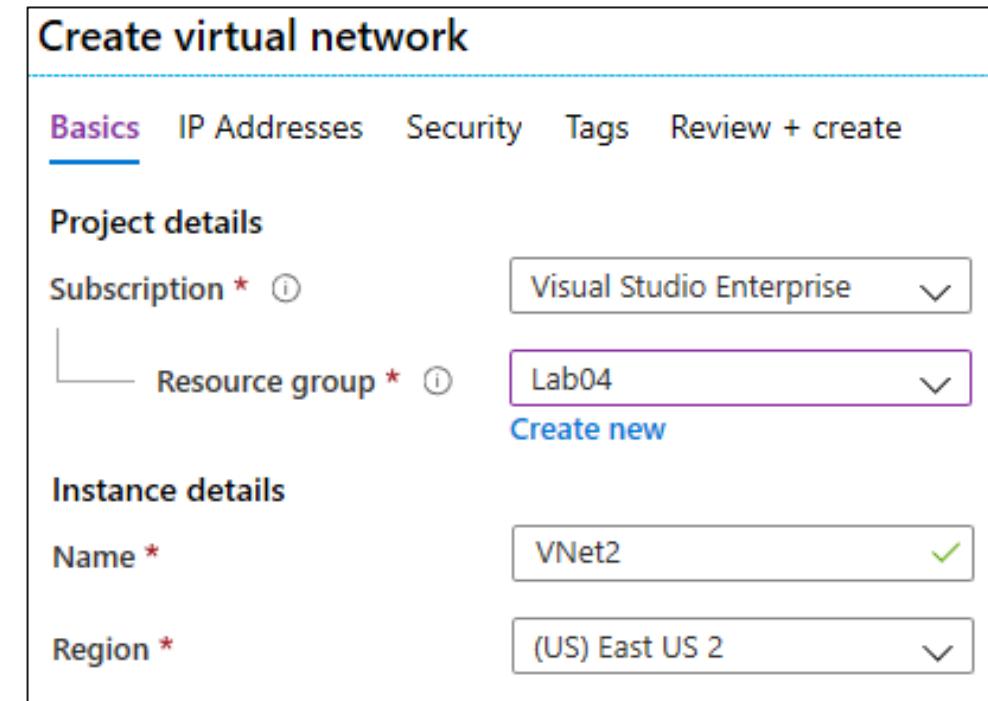
Subscription *

Resource group *

Instance details

Name *

Region *



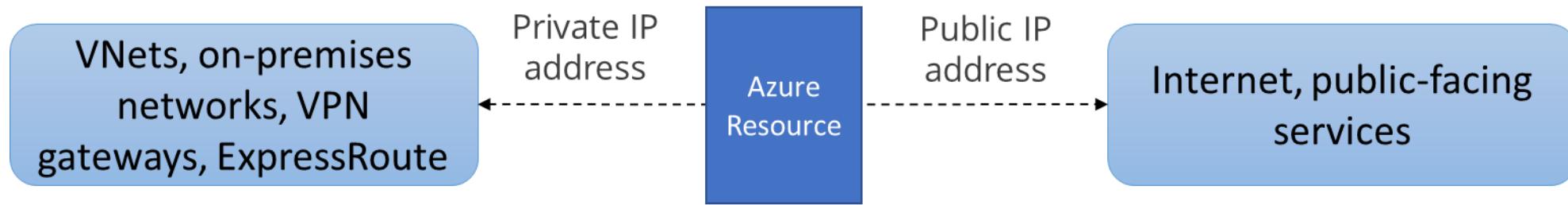
IP Addressing



IP Addressing Overview

- IP Addressing
- Creating IP Addresses
- Public IP Addresses
- Private IP Addresses

IP Addressing



- Private IP addresses are 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 are 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

Create public IP address

IP Version *

IPv4 IPv6 Both

SKU *

Basic Standard

IPv4 IP Address Configuration

Name *

IP address assignment *

Dynamic Static

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	Yes*
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

Network Security Groups



Network Security Groups Overview

- Network Security Groups
- NSG Rules
- NSG Effective Rules
- Creating NSG Rules
- Application Security Groups

Network Security Groups

The screenshot shows the Azure portal interface for a Network Security Group named 'nsg0'. The left sidebar includes options for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area displays the NSG's properties: Resource group (rg01), Location (East US), Subscription (change), Subscription ID, and Tags (Click here to add tags). It also shows associated resources: Custom security rules (1 inbound, 0 outbound), Associated with (1 subnets, 0 network interfaces), and a 'Move' button.

- 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

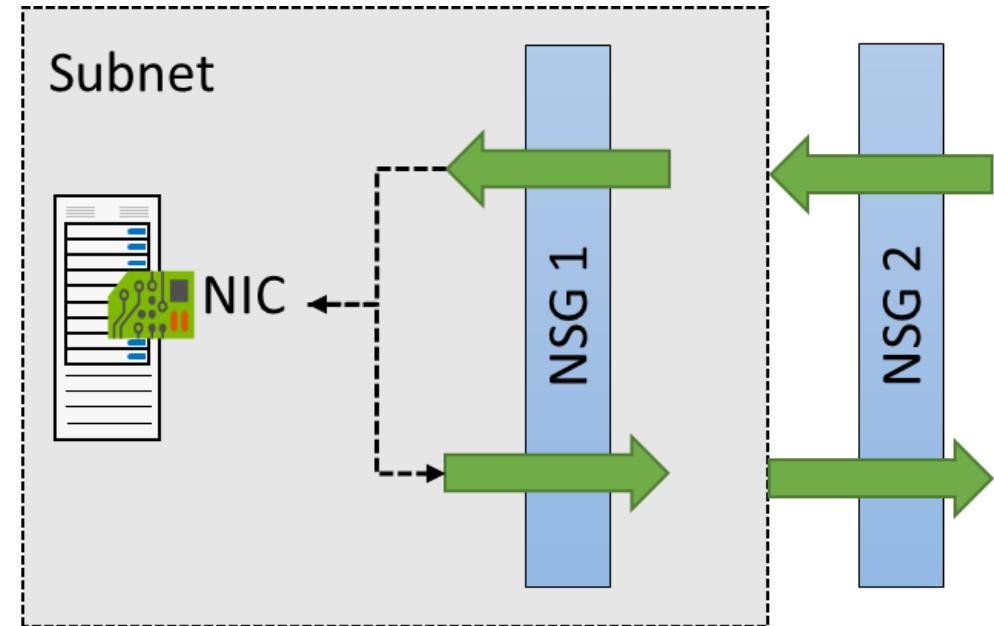
NSG Rules

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



Network Interface: [vm01990](#)

Virtual network/subnet: [vnet01/subnet0](#)

[Effective security rules](#)

NIC Public IP: -

[Topology](#)

NIC Private IP: **10.1.0.4**

Accelerated networking: **Disabled**

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

Add inbound security rule X

nsg1

Advanced

Service ⓘ

Custom

Port ranges * ⓘ

8080

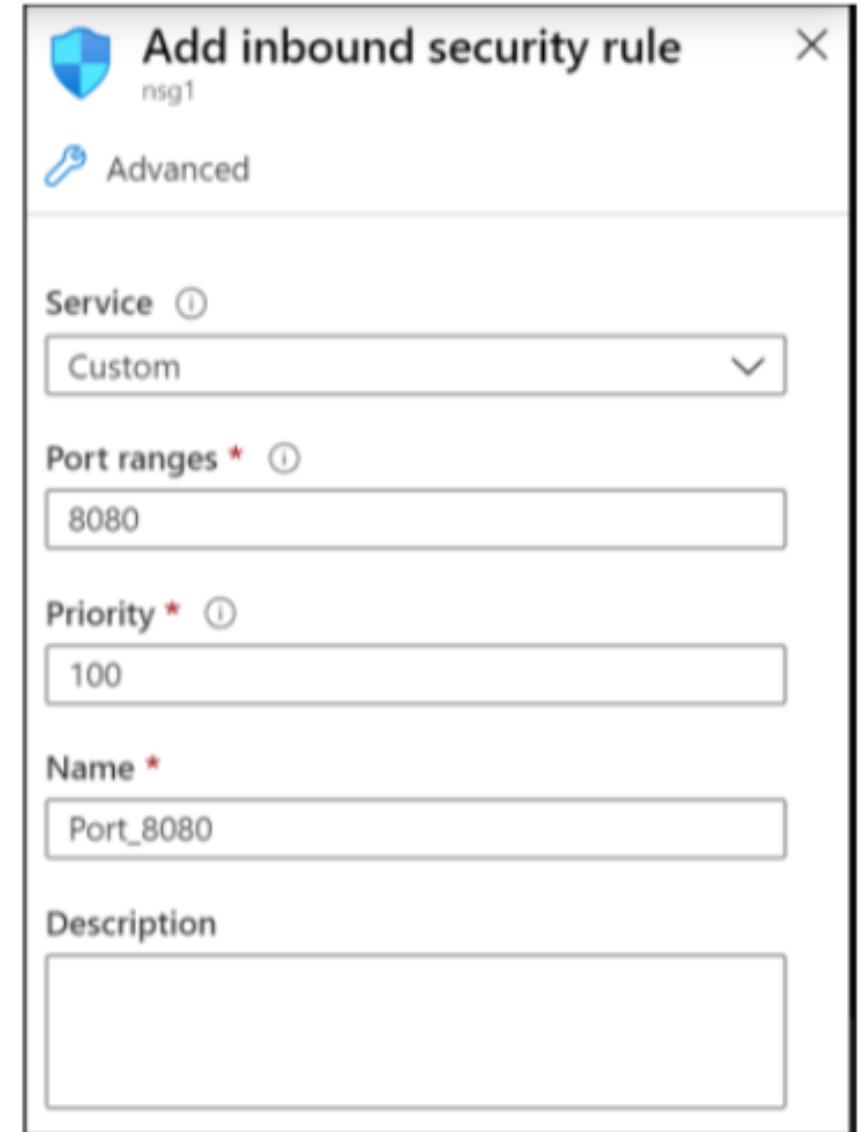
Priority * ⓘ

100

Name *

Port_8080

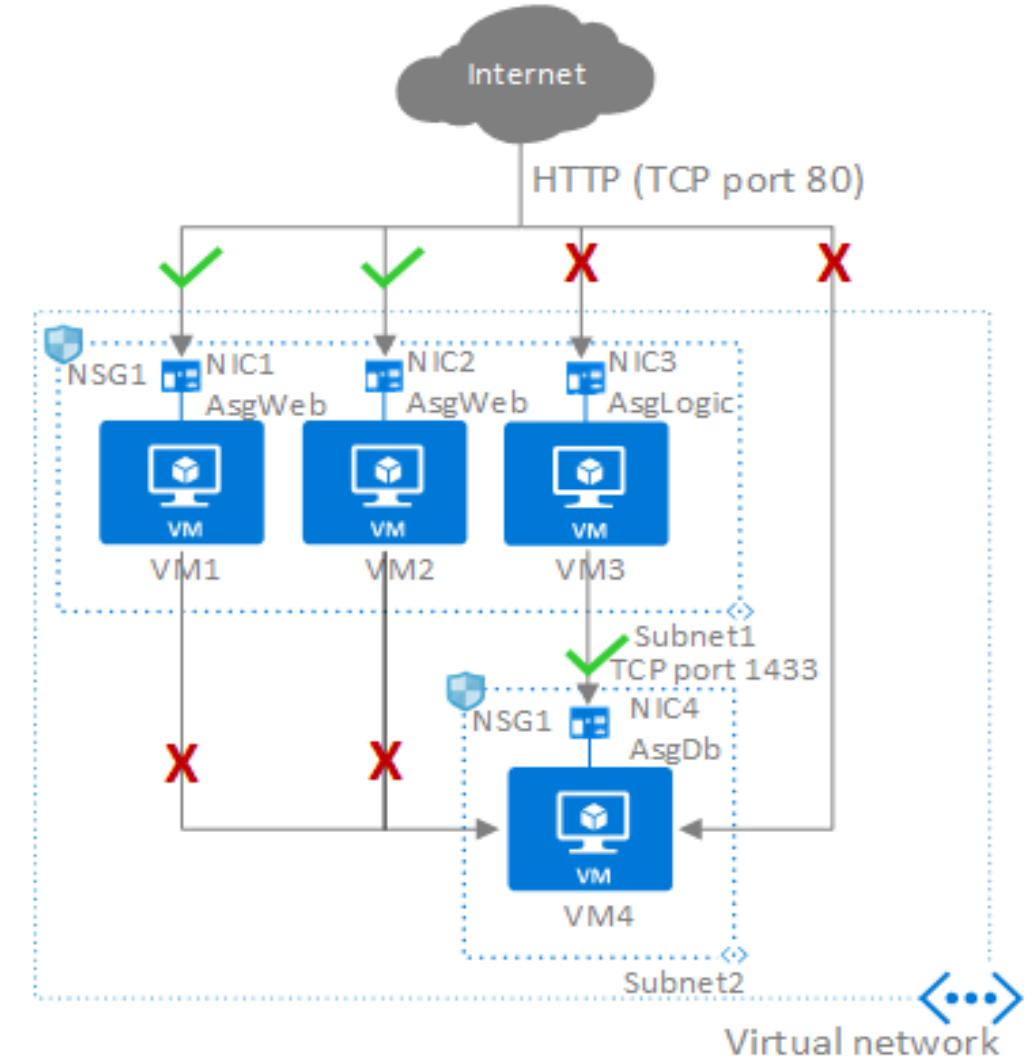
Description



Application Security Groups

Provides for the grouping of servers with similar port filtering requirements, and group together servers with similar functions, such as web servers.

- Allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses.
- Handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.



Azure Firewall

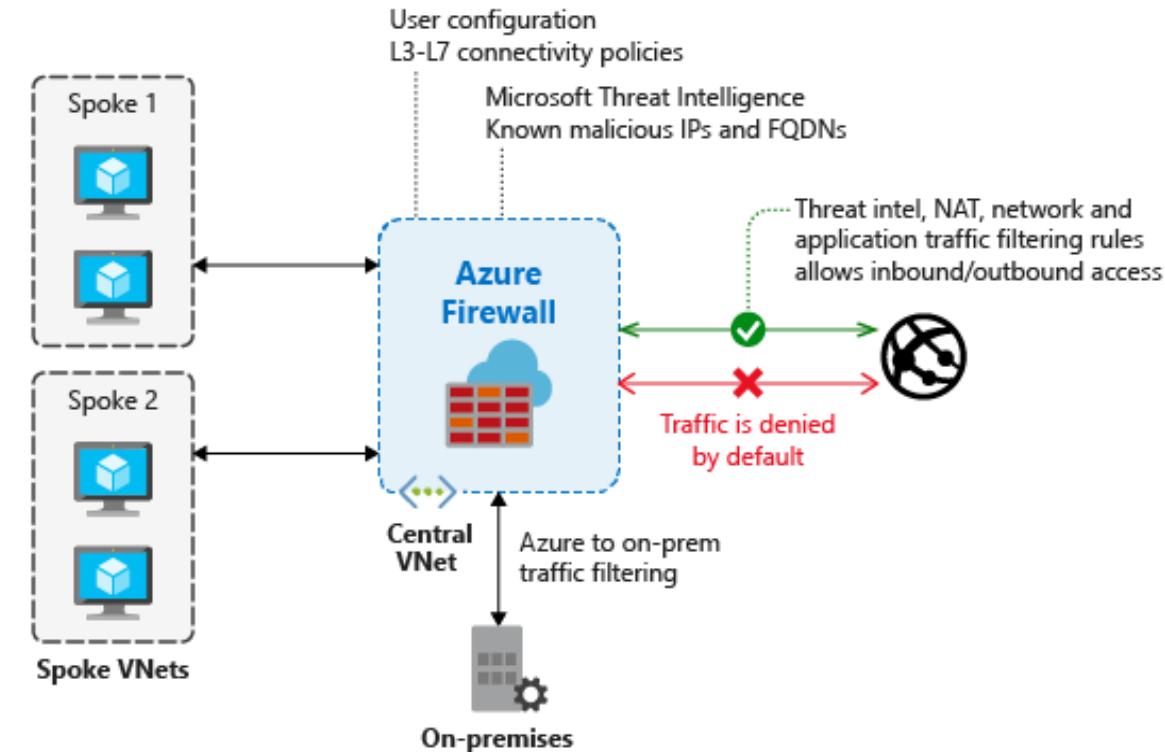


Azure Firewall Overview

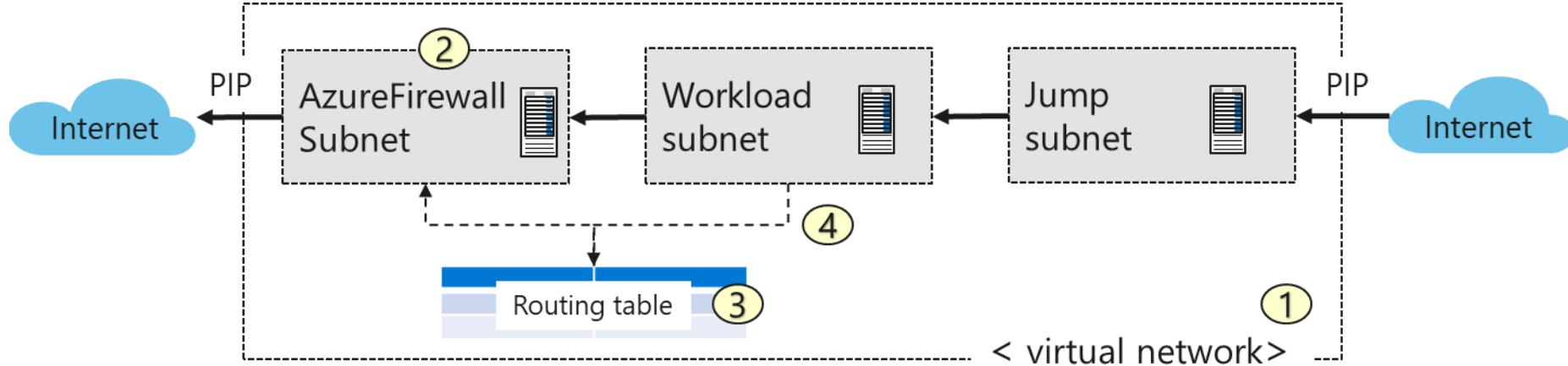
- Azure Firewall
- Implementing Firewalls
- Firewall Rules

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

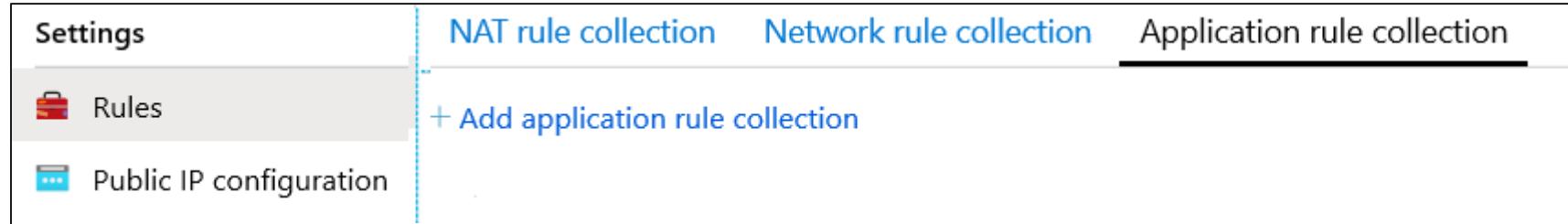


Implementing Firewalls



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

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)

Create a directory
Azure Active Directory

Basics * Configuration * Review + create

Directory details
Configure your new directory

Organization name * *Azure Administrator Incorporated*

Initial domain name * *azureadminincorg* *azureadminincorg.onmicrosoft.com*

Country/Region *United States*

Review + create < Previous Next : Review + create >



Custom domain name
Azure Administrator Incorporated

Custom domain name * *azureadmininc.org*

Add domain

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

The screenshot shows the Azure portal interface for verifying a custom domain. The domain name 'azureadmininc.org' is displayed at the top, along with a 'Delete' button and a 'Got feedback?' link. A message box contains an informational icon and text: 'To use azureadmininc.org with your Azure AD, create a new TXT record with your domain name registrar using the info below.' Below this, there are fields for configuration:

- Record type:** A radio button is selected for 'TXT'.
- Alias or host name:** The value '@' is entered.
- Destination or points to address:** The value 'MS=ms79094380' is entered.
- TTL:** The value '3600' is entered.

At the bottom, there is a link 'Share these settings via email' and a note: 'Verification will not succeed until you have configured your domain with your registrar as described above.'

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
- Only one set of addresses can be configured with the domain name registrar

Create DNS zone X

[Basics](#) [Tags](#) [Review + create](#)

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

Project details

Subscription * ▼

Resource group * ▼
[Create new](#)

Instance details

Name * ✓

Resource group location ? ▼

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

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

The screenshot shows the Azure DNS Zone Management interface for the domain 'azureadmininc.org'. The top navigation bar includes a 'DNS' icon, the domain name 'azureadmininc.org', and a 'DNS zone' label. Below the navigation are standard actions: '+ Record set', 'Move', 'Delete zone', and 'Refresh'. The main content area displays several configuration details:

- Resource group ([change](#)): rg-dns
- Subscription ([change](#)): MSDN Platforms Subscription
- Subscription ID
- Tags ([change](#)): Click here to add tags

On the right side, there is a list of four name servers:

- Name server 1: ns1-02.azure-dns.com.
- Name server 2: ns2-02.azure-dns.net.
- Name server 3: ns3-02.azure-dns.org.
- Name server 4: ns4-02.azure-dns.info.

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

Add record set

azurereadadmininc.org

Name

helloworld .azurereadadmininc.org

Type

A

Alias record set i

Yes No

TTL *

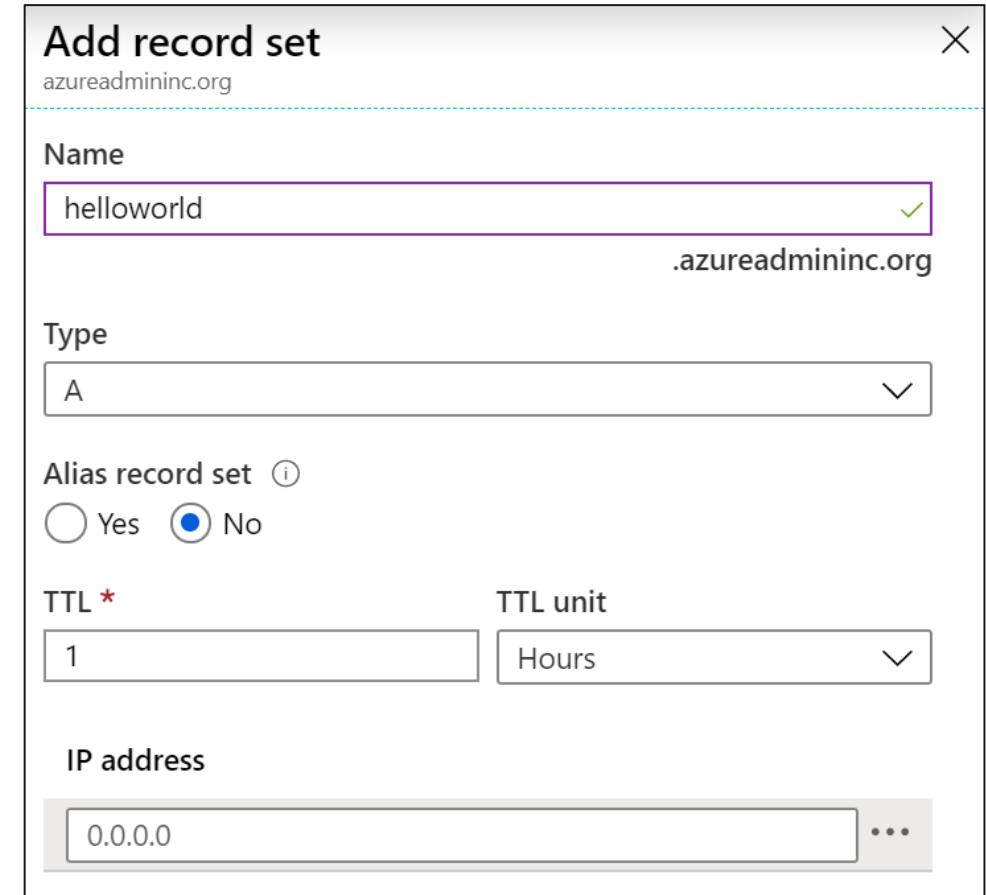
1

TTL unit

Hours

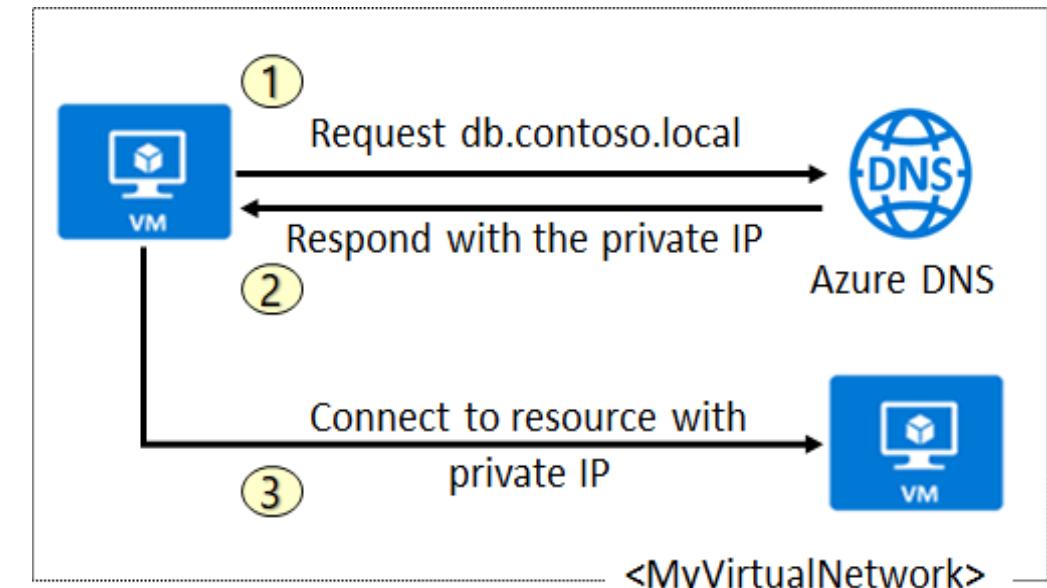
IP address

0.0.0.0 ...

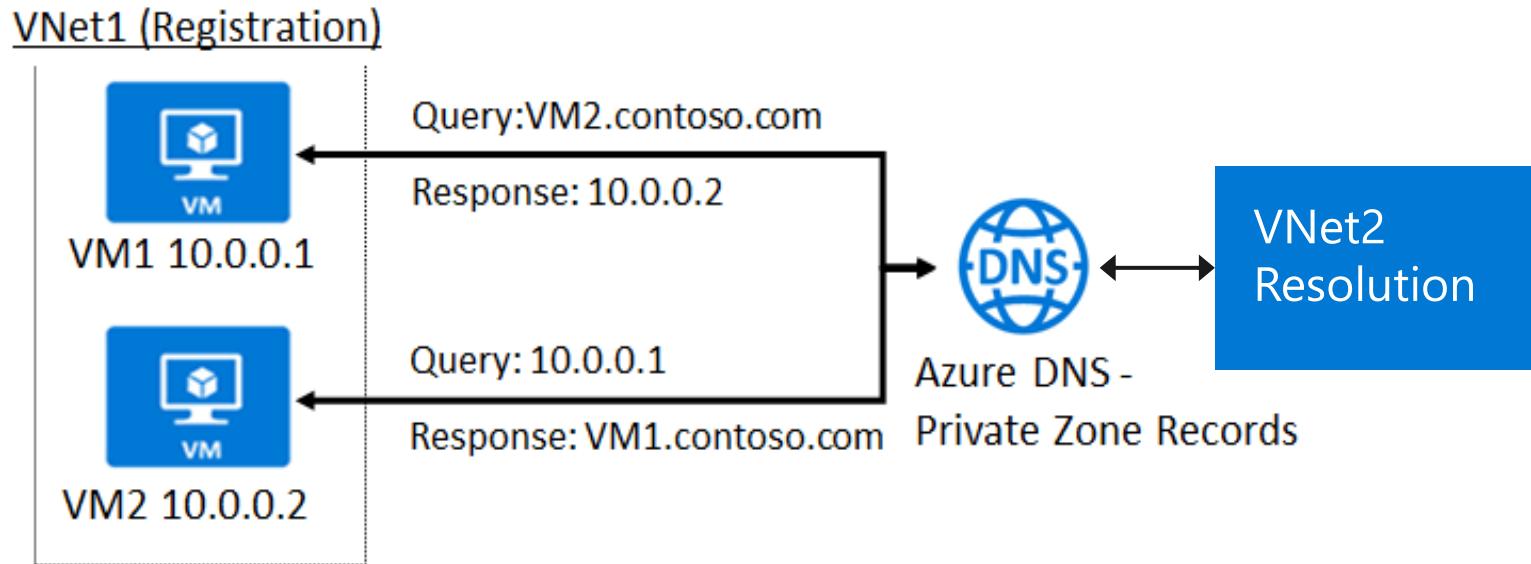


DNS for Private Domains

- 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

Module 04 Lab and Review



Lab 04 - Implement Virtual Networking

Lab scenario

You plan to create a virtual network in Azure that will host a couple of Azure virtual machines. You will deploy them into different subnets of the virtual network. You also want to ensure that their private and public IP addresses will not change over time. To comply with Contoso security requirements, you need to protect public endpoints of Azure virtual machines accessible from Internet. Finally, you need to implement DNS name resolution for Azure virtual machines both within the virtual network and from Internet.

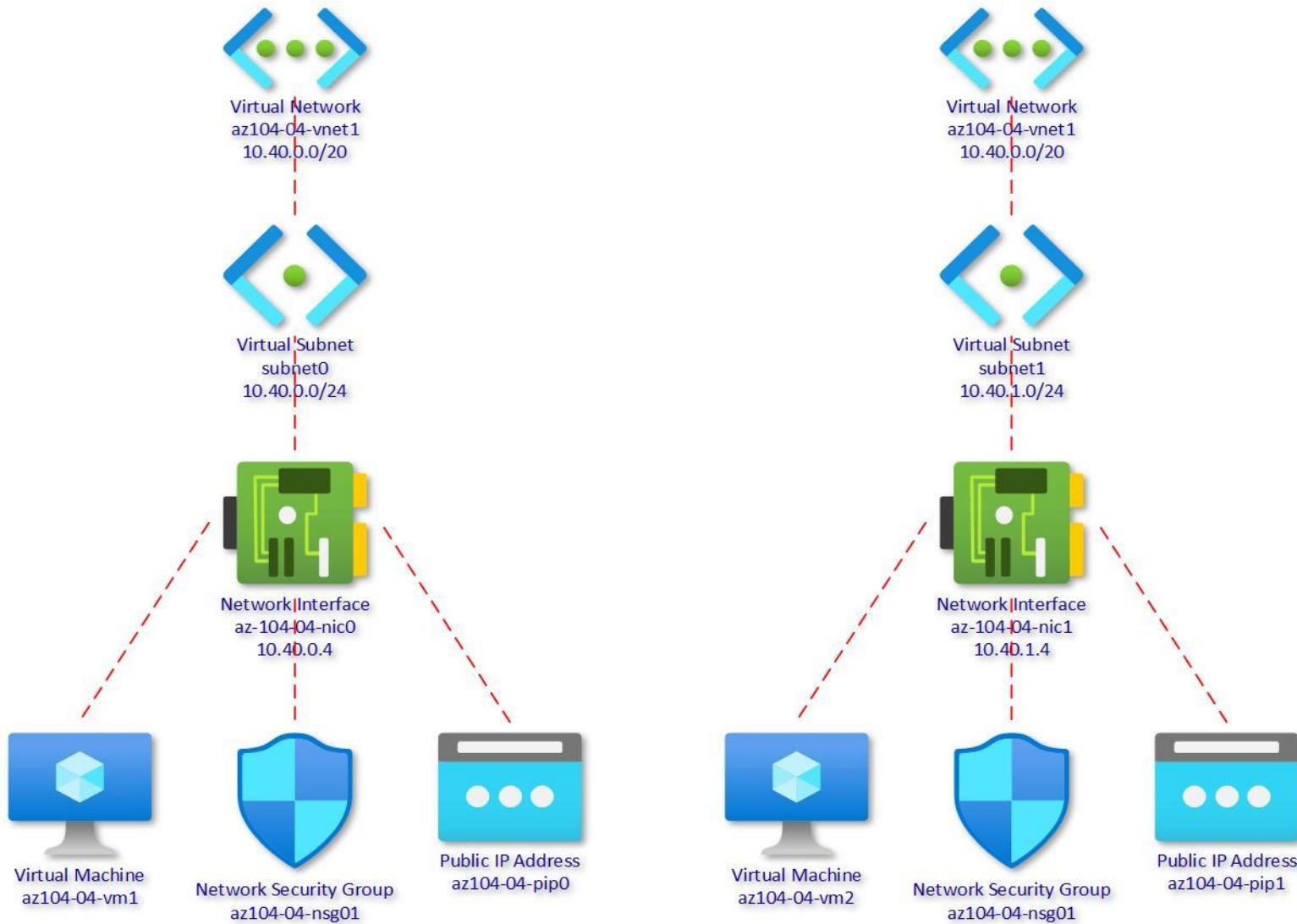
Objectives

- Task 1: Create and configure a virtual network
- Task 2: Deploy virtual machines into the virtual network
- Task 3: Configure private and public IP addresses of Azure VMs
- Task 4: Configure network security groups
- Task 5: Configure Azure DNS for internal name resolution
- Task 6: Configure Azure DNS for external name resolution

Next slide for
an architecture diagram



Lab 04 – Architecture Diagram



AZ-104T00A

Module 05:

Intersite Connectivity



Module Overview

- VNet Peering
- VPN Gateway Connections
- ExpressRoute and Virtual WAN

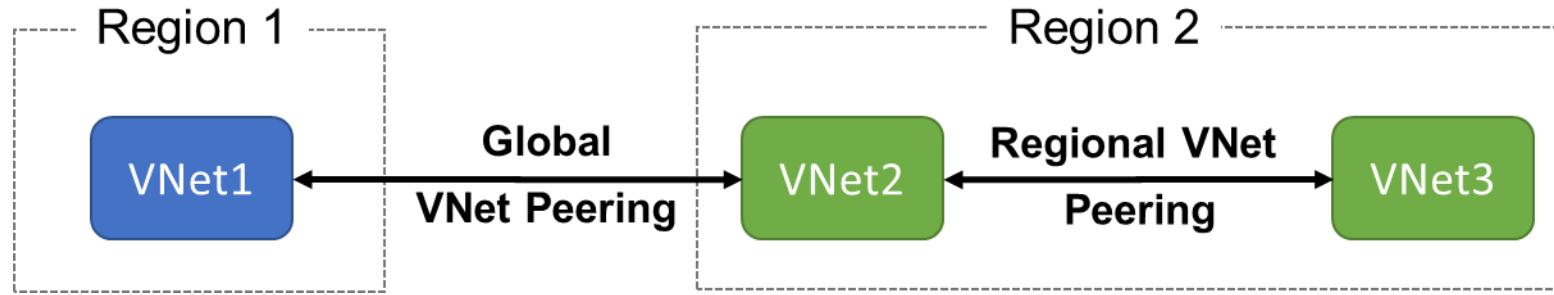
VNet Peering



VNet Peering Overview

- VNet Peering
- Gateway Transit and Connectivity
- Configure VNet Peering
- Service Chaining

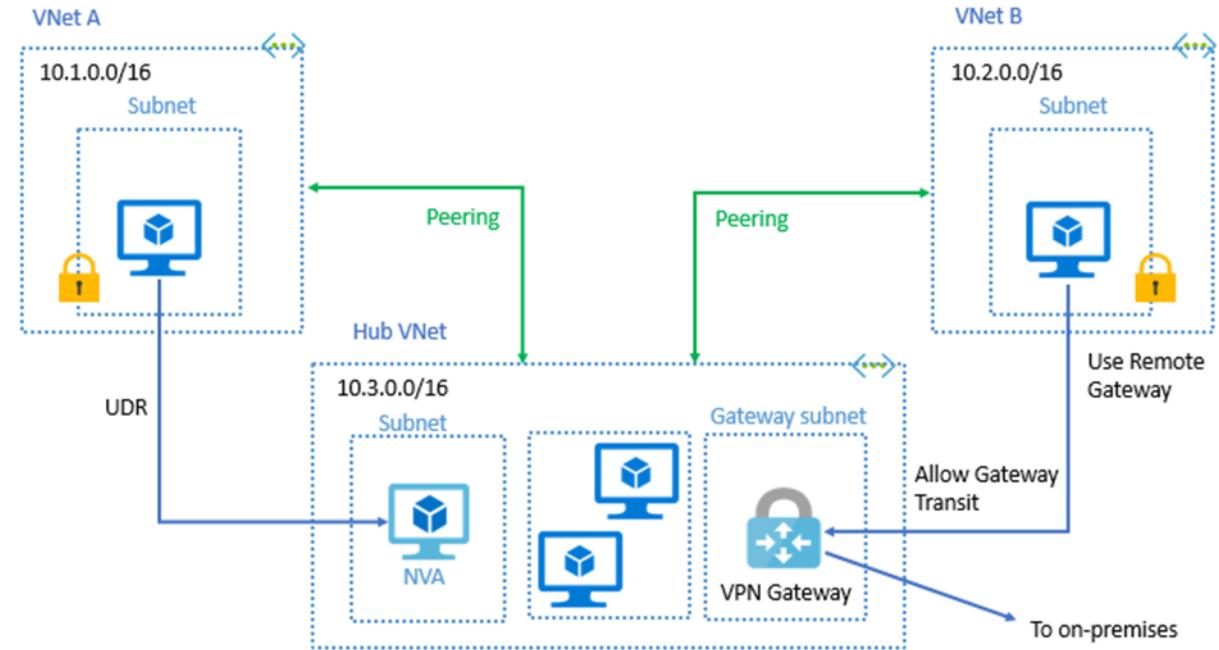
VNet Peering



- 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 -only one virtual network can have this enabled

Configuration

Configure virtual network access settings

Allow virtual network access from vnet1 to vnet2 ⓘ

Configure forwarded traffic settings

Allow forwarded traffic from vnet2 to vnet1 ⓘ

Configure gateway transit settings

Allow gateway transit ⓘ

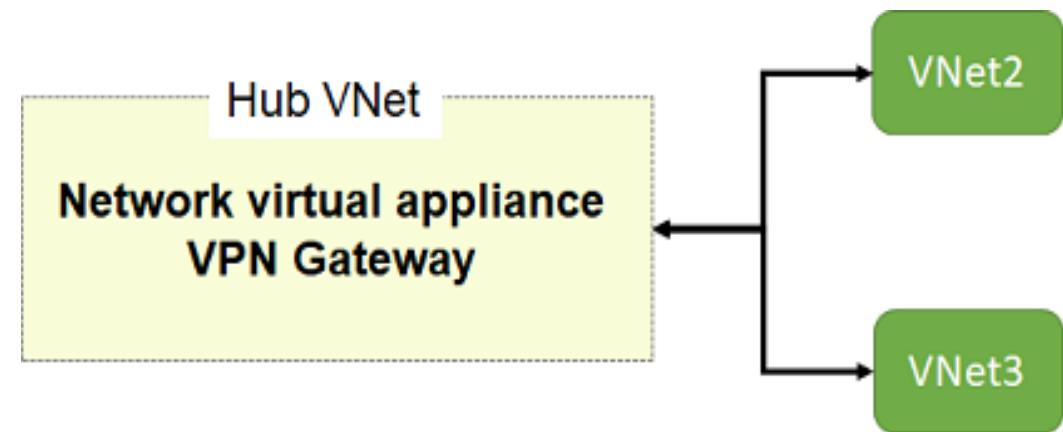
Configure Remote Gateways settings

Use remote gateways ⓘ

✓ 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



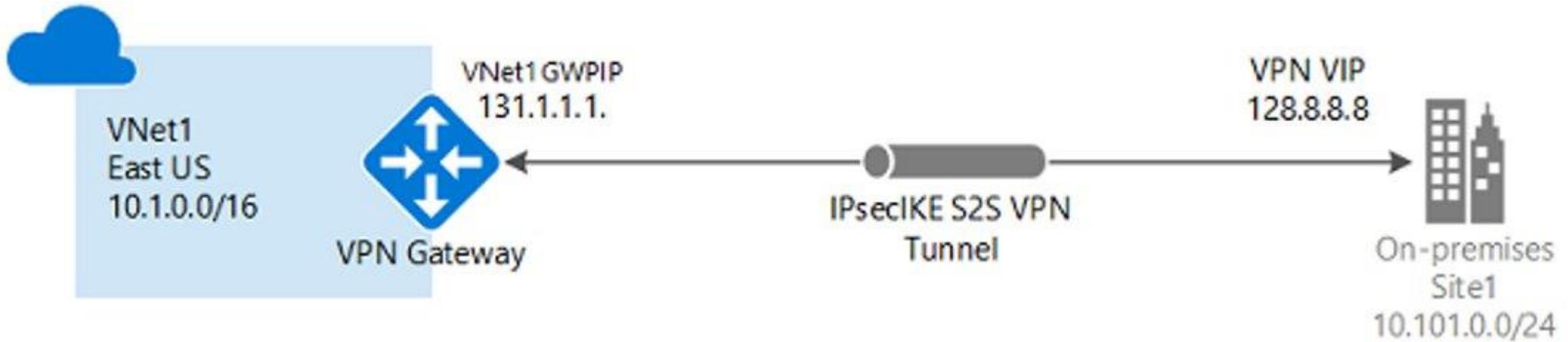
VPN Gateway Connections



VPN Gateway Connections Overview

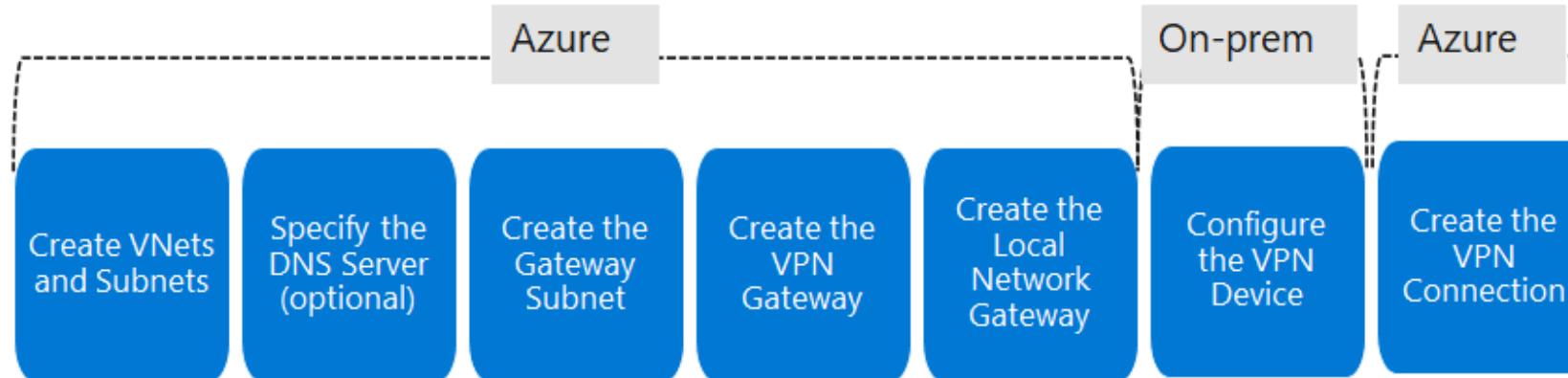
- VPN Gateways
- Implement Site-to-Site VPN Connections
- Create the Gateway Subnet
- VPN Gateway Configuration
- VPN Gateway Types
- VPN Gateway SKU and Generation
- Create the Local Network Gateway
- Configure the On-Premises VPN Device
- Create the VPN Connection
- High Availability Scenarios

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

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

Create virtual network gateway

Instance details

Name *

Region * (US) East US

Gateway type * VPN ExpressRoute

VPN type * Route-based Policy-based

SKU * VpnGw1

Generation Generation1

VIRTUAL NETWORK

Virtual network *

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Enable active-active mode * Enabled Disabled

Configure BGP ASN * Enabled Disabled

✓ 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

SKU * ⓘ VpnGw1

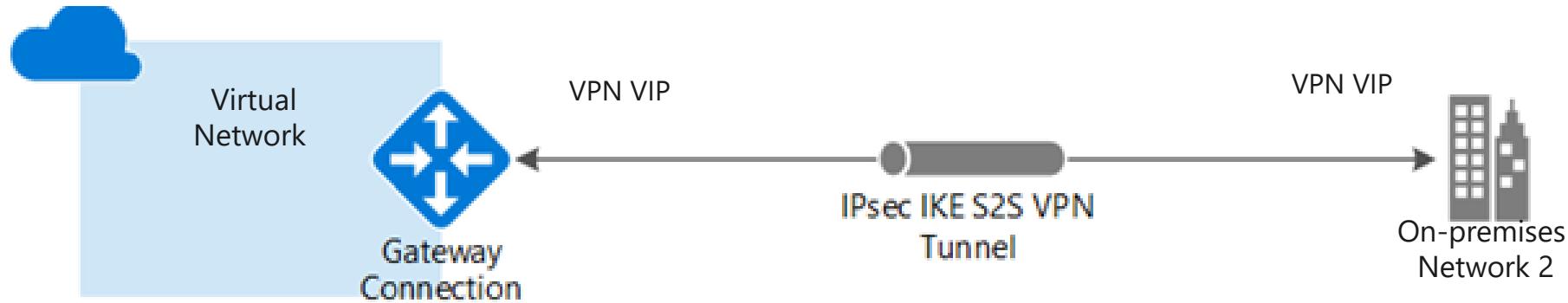
Generation ⓘ Generation1

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

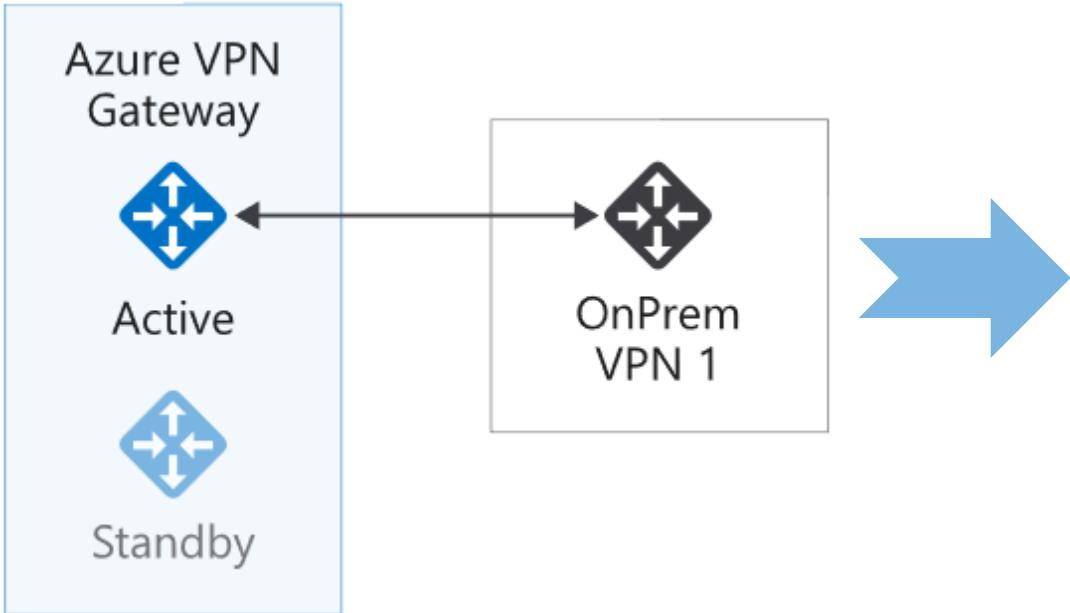
Configure the On-Premises VPN Device



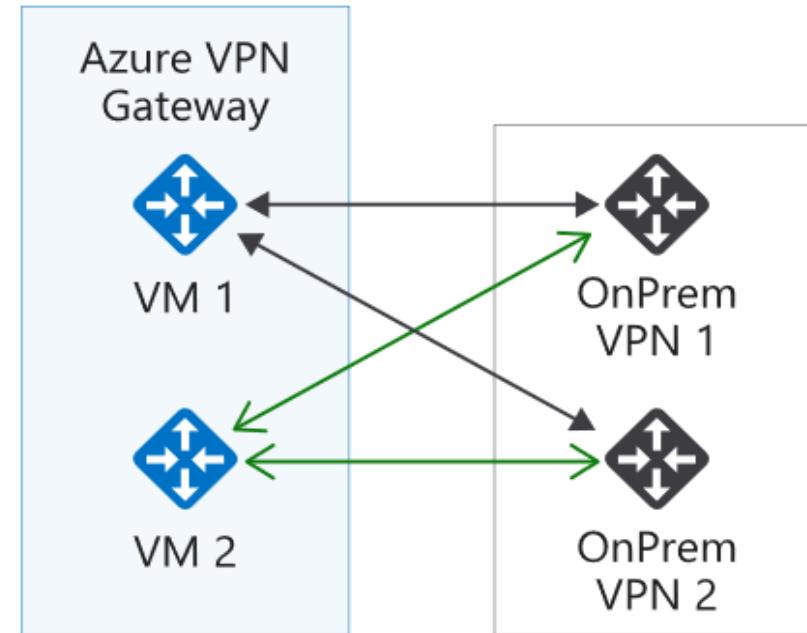
- Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)
- A VPN device configuration script may be available
- Remember the shared key for the Azure connection (next step)
- Specify the public IP address (previous step)

High Availability Scenarios

Active/standby (default)



Active/active



- VPN gateways are deployed as two instances
- Enable active/active mode for higher availability

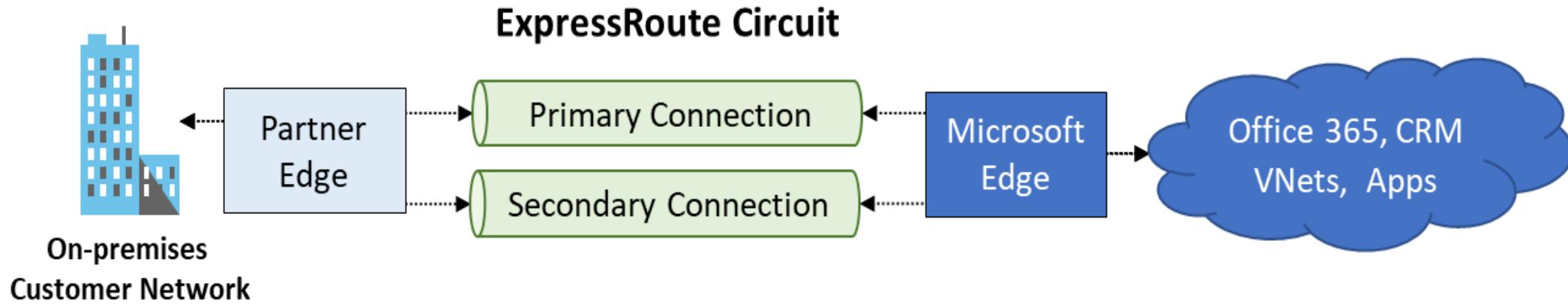
ExpressRoute and Virtual WAN



ExpressRoute and Virtual WAN Overview

- ExpressRoute
- ExpressRoute Capabilities
- Coexisting Site-to-Site and ExpressRoute
- Intersite Connection Comparisons
- Virtual WANs

ExpressRoute



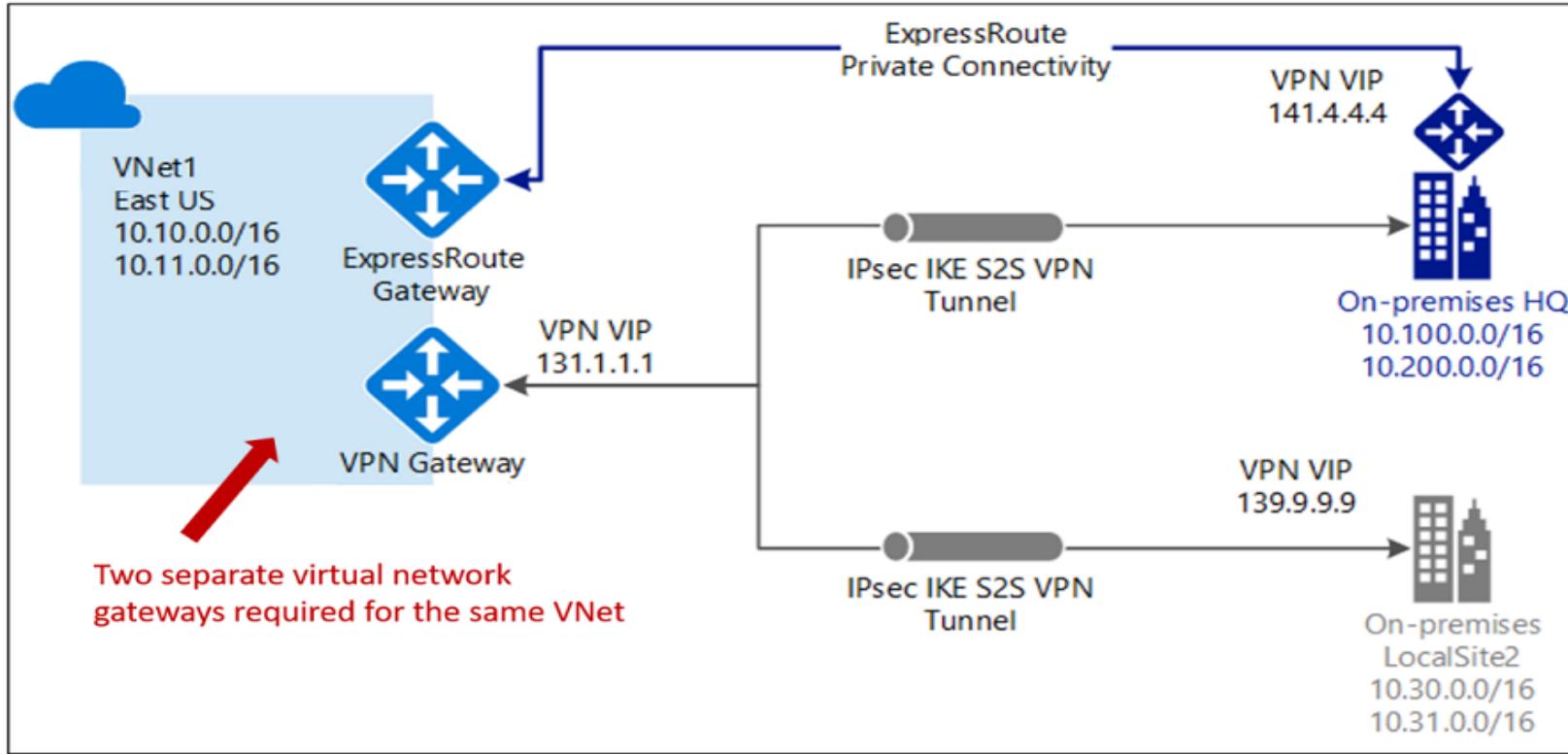
- Private connections between your on-premises network and Microsoft datacenters
- Connections do not go over the public Internet – partner network
- Secure, reliable, low latency, high speed connections

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



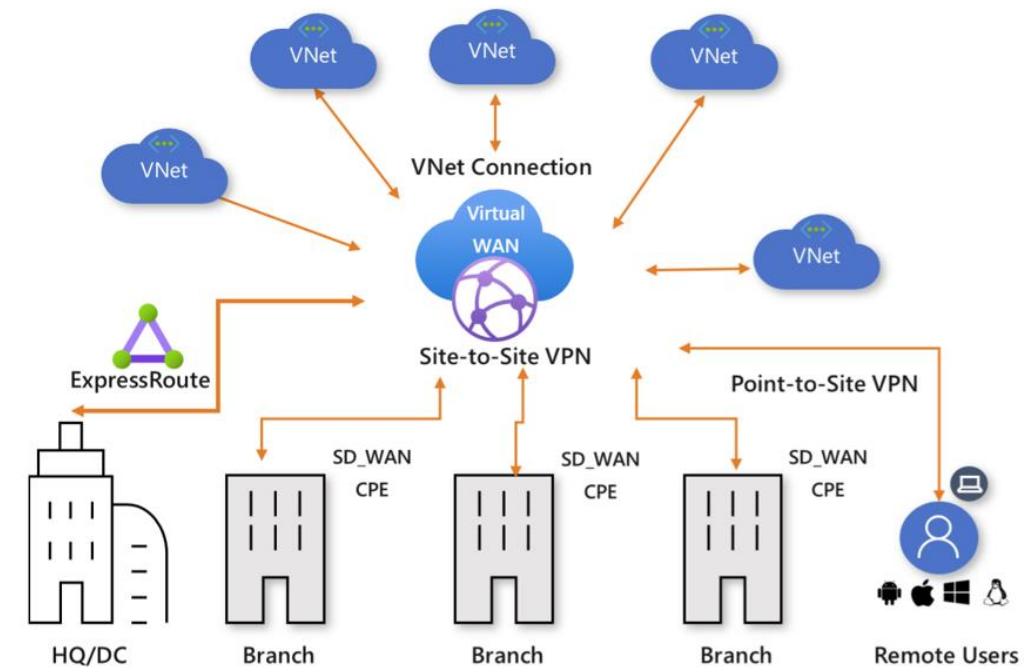
- Use S2S VPN as a secure failover path for ExpressRoute
- Use S2S VPNs to connect to sites that are not connected with ExpressRoute
- Notice two VNet gateways for the same virtual network

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



Module 05 Lab and Review



Lab 05 - Implement Intersite Connectivity

Lab scenario

Contoso has its datacenters in Boston, New York, and Seattle offices connected via a mesh wide-area network links, with full connectivity between them. You need to implement a lab environment that will reflect the topology of the Contoso's on-premises networks and verify its functionality.

Objectives

Task 1: Provision the lab environment

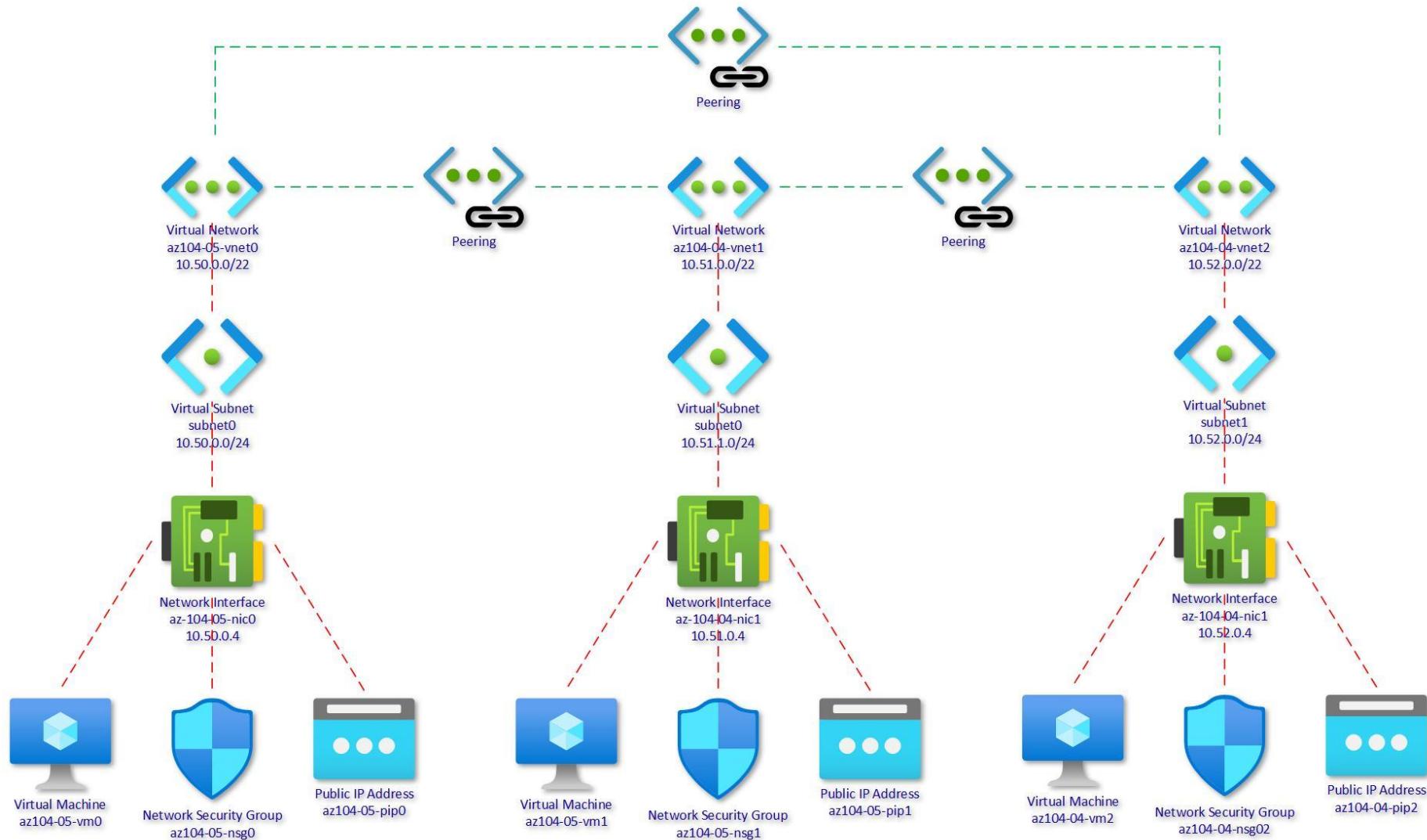
Task 2: Configure local and global virtual network peering

Task 3: Test intersite connectivity

Next slide for
an architecture diagram



Lab 05 – Architecture Diagram



AZ-104T00A

Module 06:

Network Traffic Management



Module Overview

- Network Routing and Endpoints
- Azure Load Balancer
- Application Gateway
- Traffic Manager

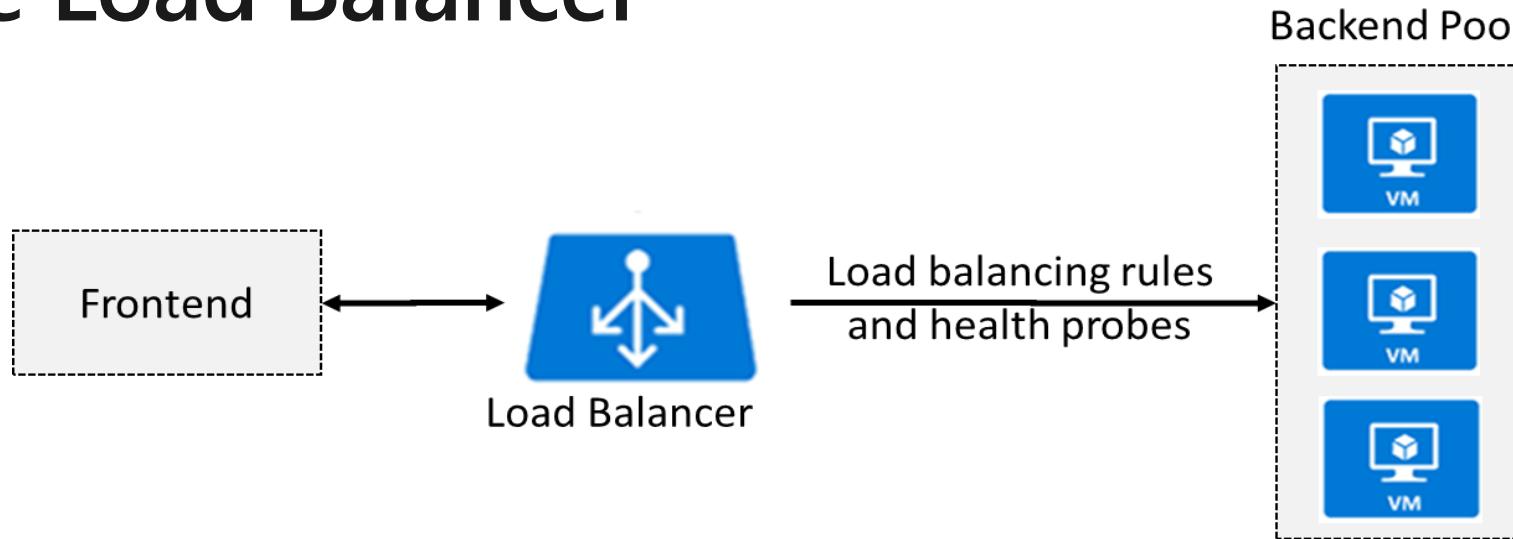
Azure Load Balancer



Azure Load Balancer Overview

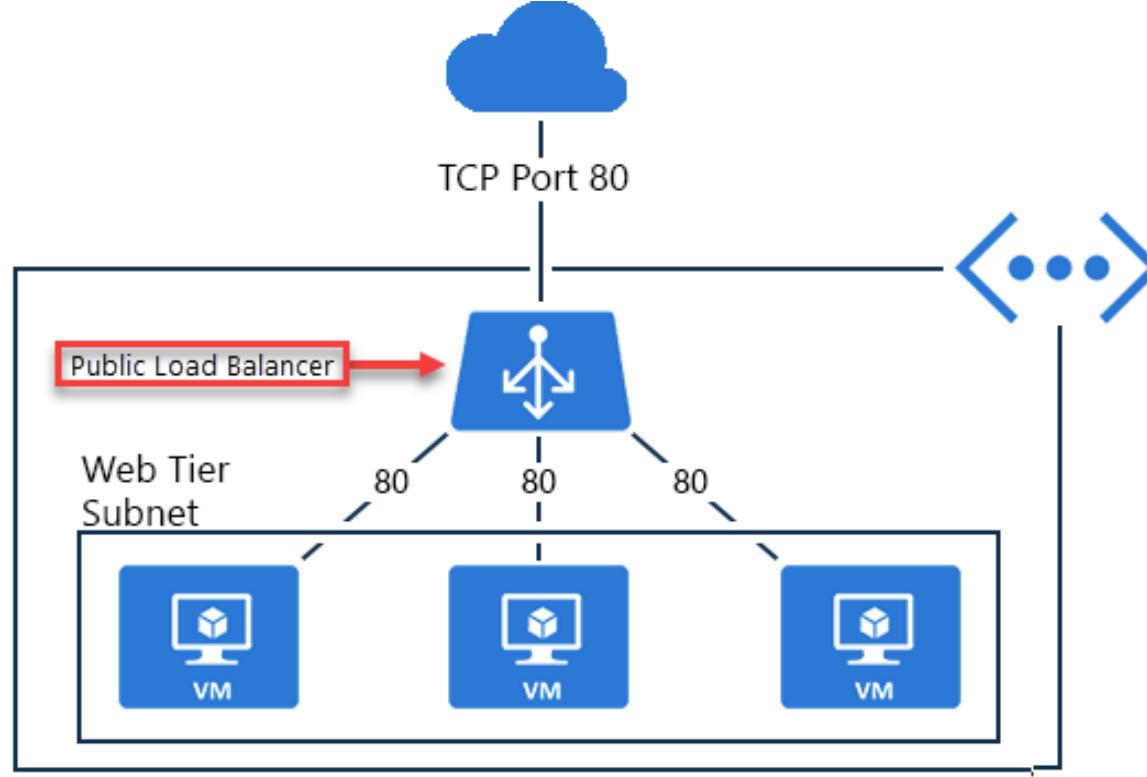
- Azure Load Balancer
- Public Load Balancer
- Internal Load Balancer
- Load Balancer SKUs
- Backend Pools
- Load Balancer Rules
- Session Persistence
- Health Probes

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

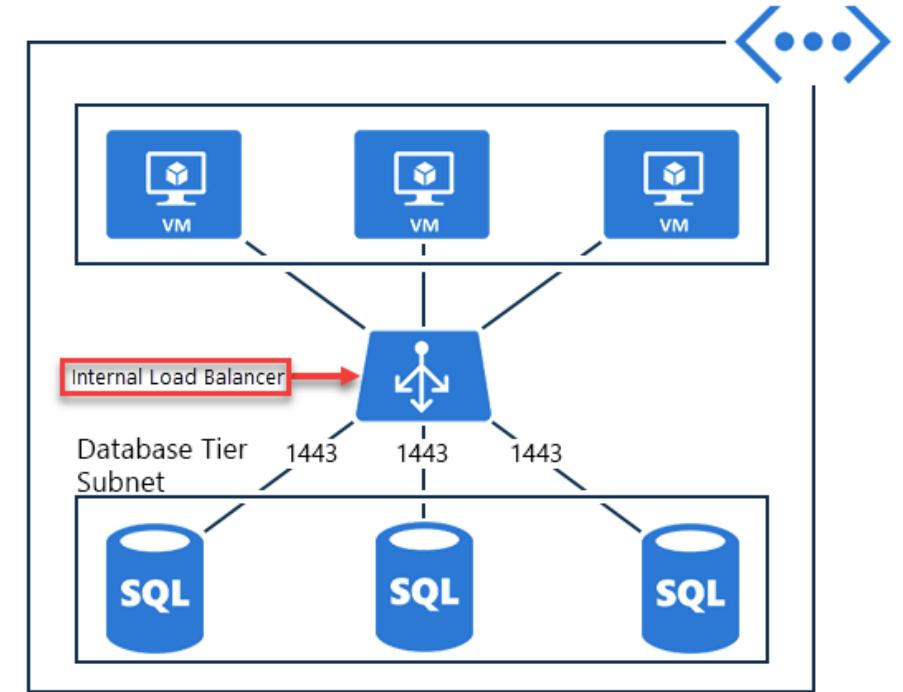
Public Load Balancer



- 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
- Load Balancer rule cannot span two virtual networks
- No charge for the Basic Load Balancer SKU

Instance details

Name * ✓

Region * ▼

Type * (i)
 Internal Public

SKU * (i)
 Basic Standard

Configure virtual network.

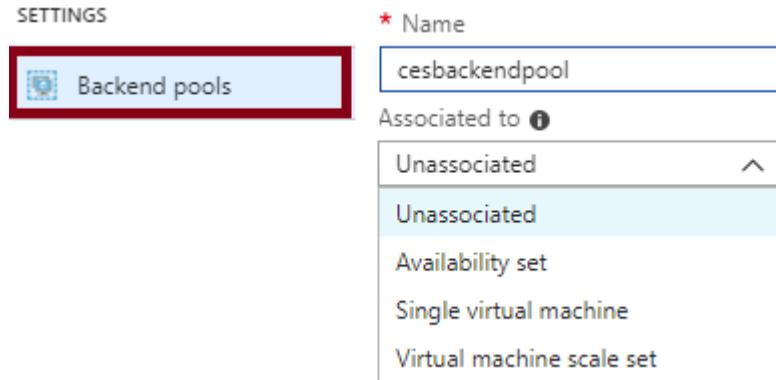
Virtual network * (i) ▼

Subnet *
 ▼

[Manage subnet configuration](#)

IP address assignment *
 Static Dynamic

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

Add load balancing rule

Ib01

Name *

 ✓

IP Version *

 IPv4 IPv6

Frontend IP address * ⓘ

 ✓

Protocol

 TCP UDP

Port *

Backend port * ⓘ

Backend pool ⓘ

 ✓

Health probe ⓘ

 ✓

Session persistence ⓘ

 ✓

Idle timeout (minutes) ⓘ

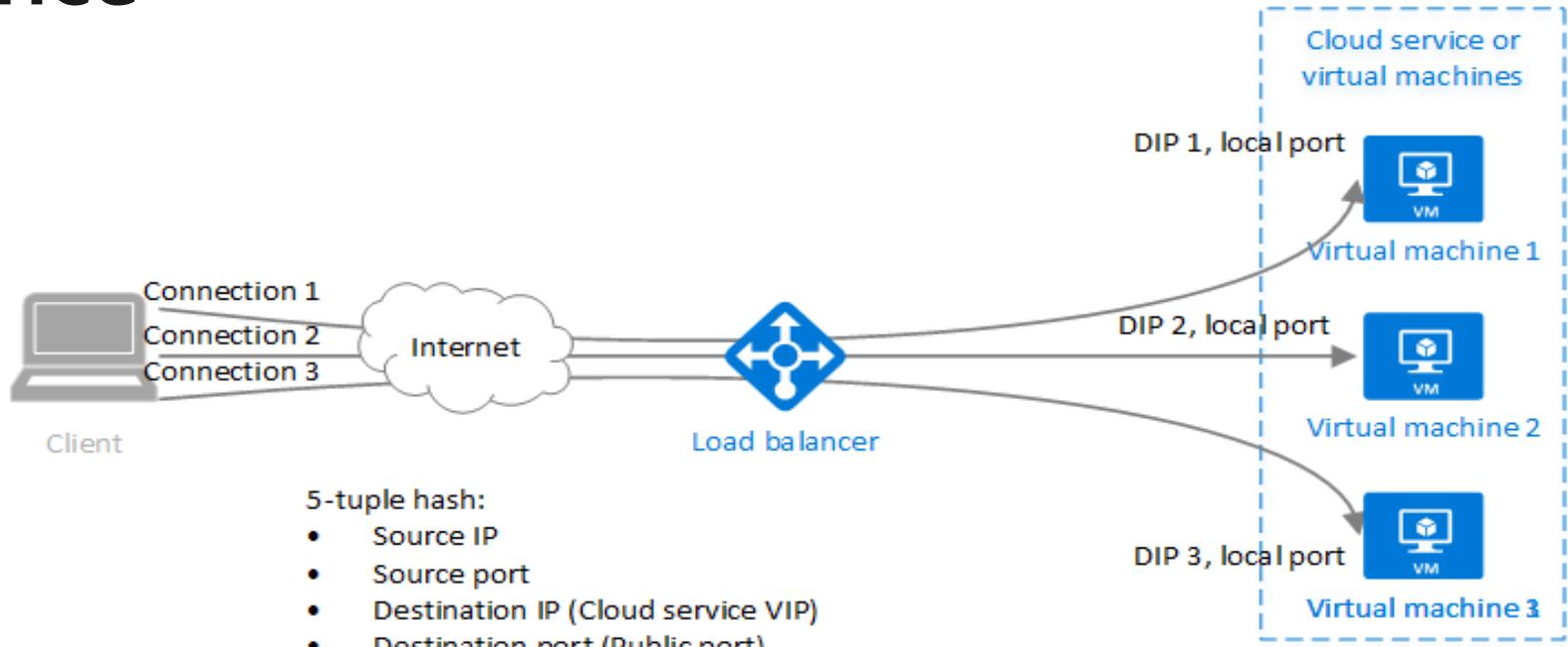
 4

Floating IP (direct server return) ⓘ

Disabled Enabled

Session Persistence

Session persistence ⓘ
None
None
Client IP
Client IP and protocol



- 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

Add health probe
lb01

Name *
hp01

Protocol ⓘ
HTTP

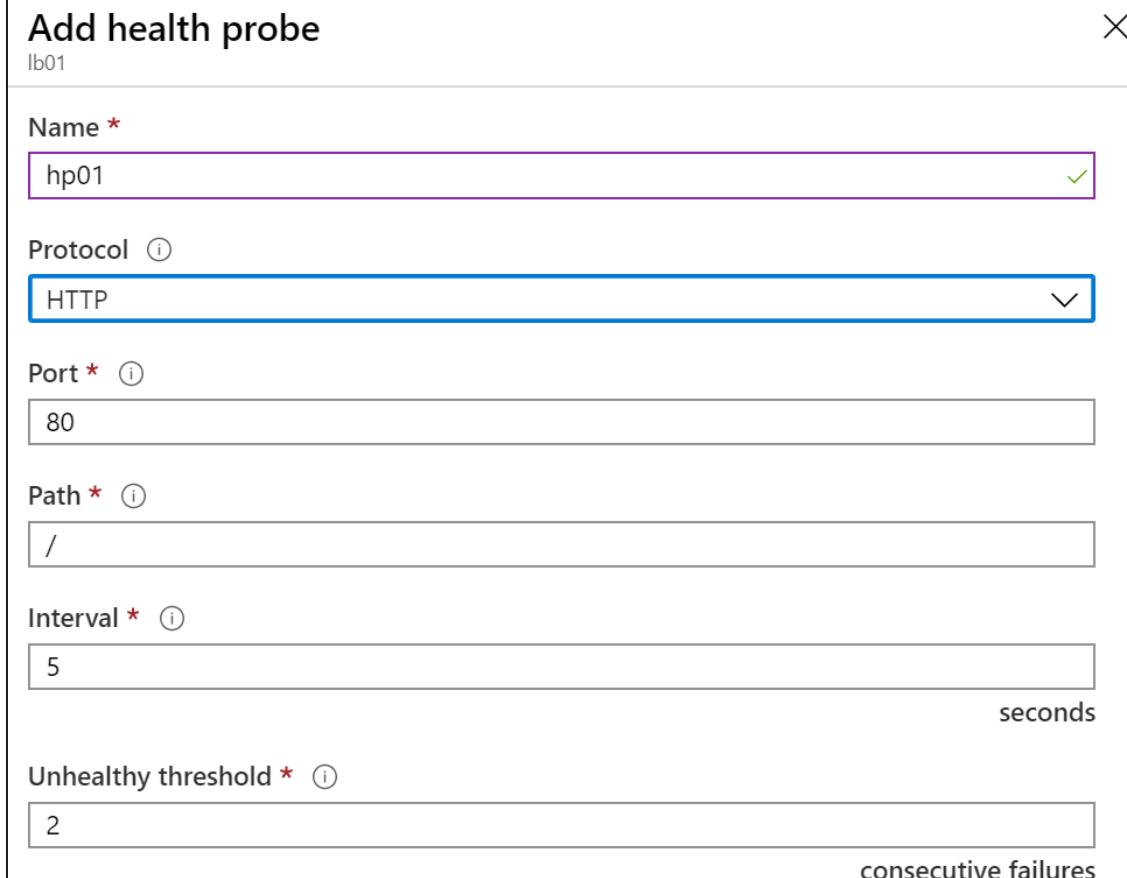
Port * ⓘ
80

Path * ⓘ
/

Interval * ⓘ
5 seconds

Unhealthy threshold * ⓘ
2 consecutive failures

X



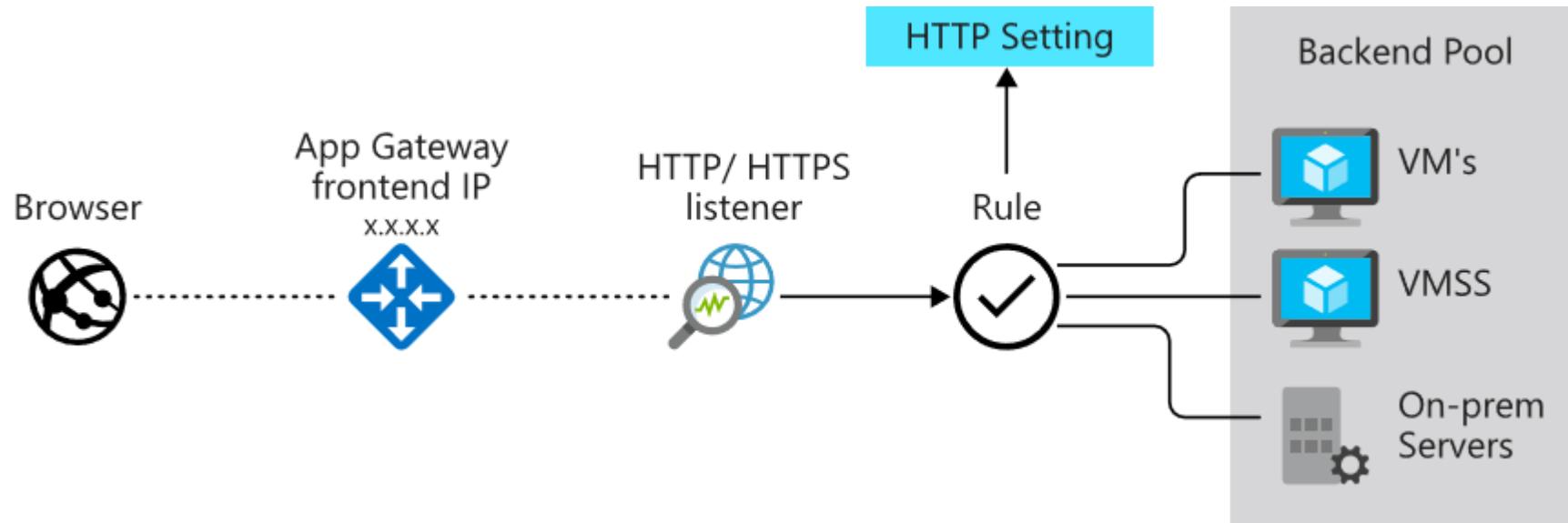
Azure Application Gateway



Application Gateway Overview

- Application Gateway
- Application Gateway Routing
- Application Gateway Configuration

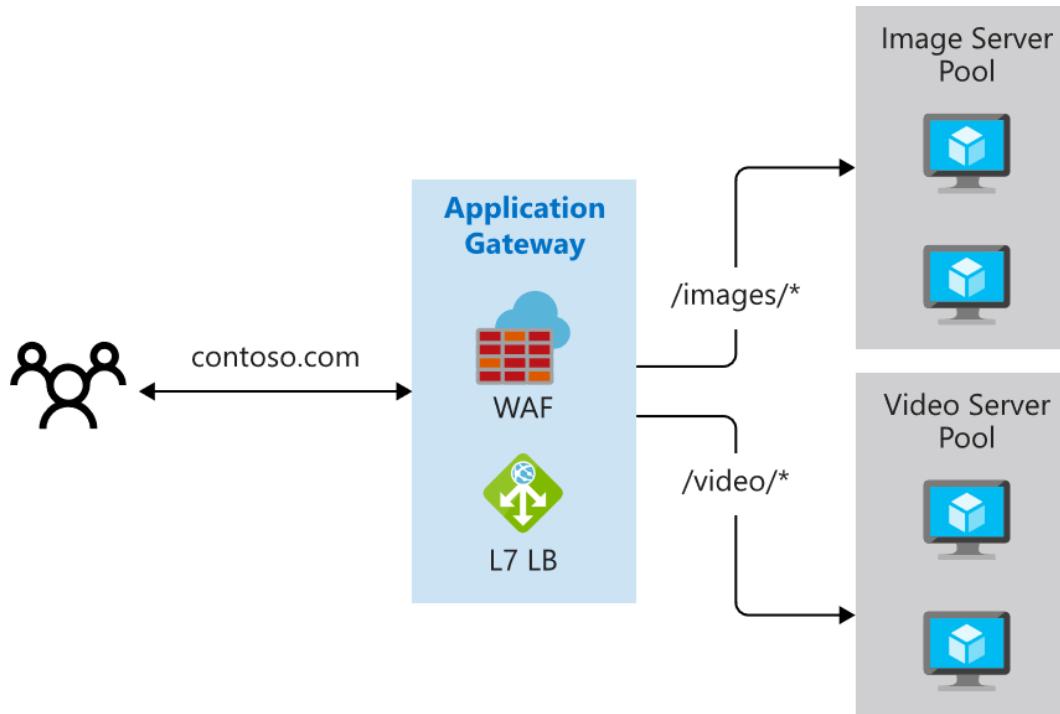
Application Gateway



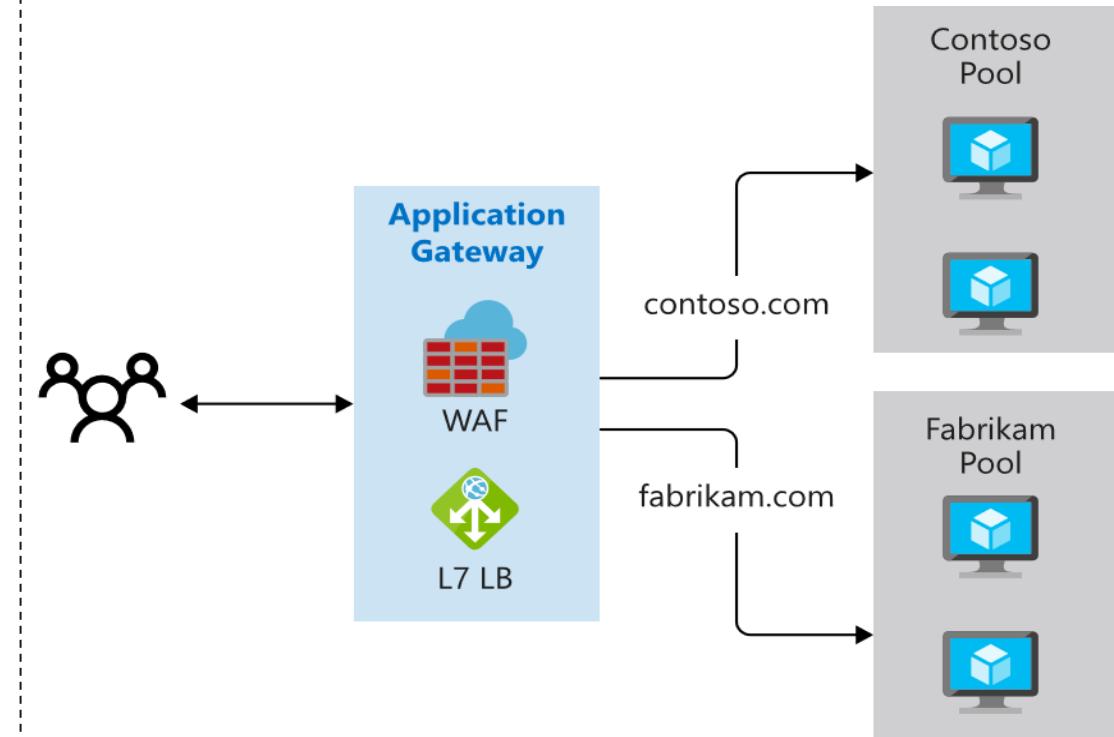
- Manages web app requests
- Routes traffic to a pool of web servers based on the URL of a request
- The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Application Gateway Routing

Path-based routing

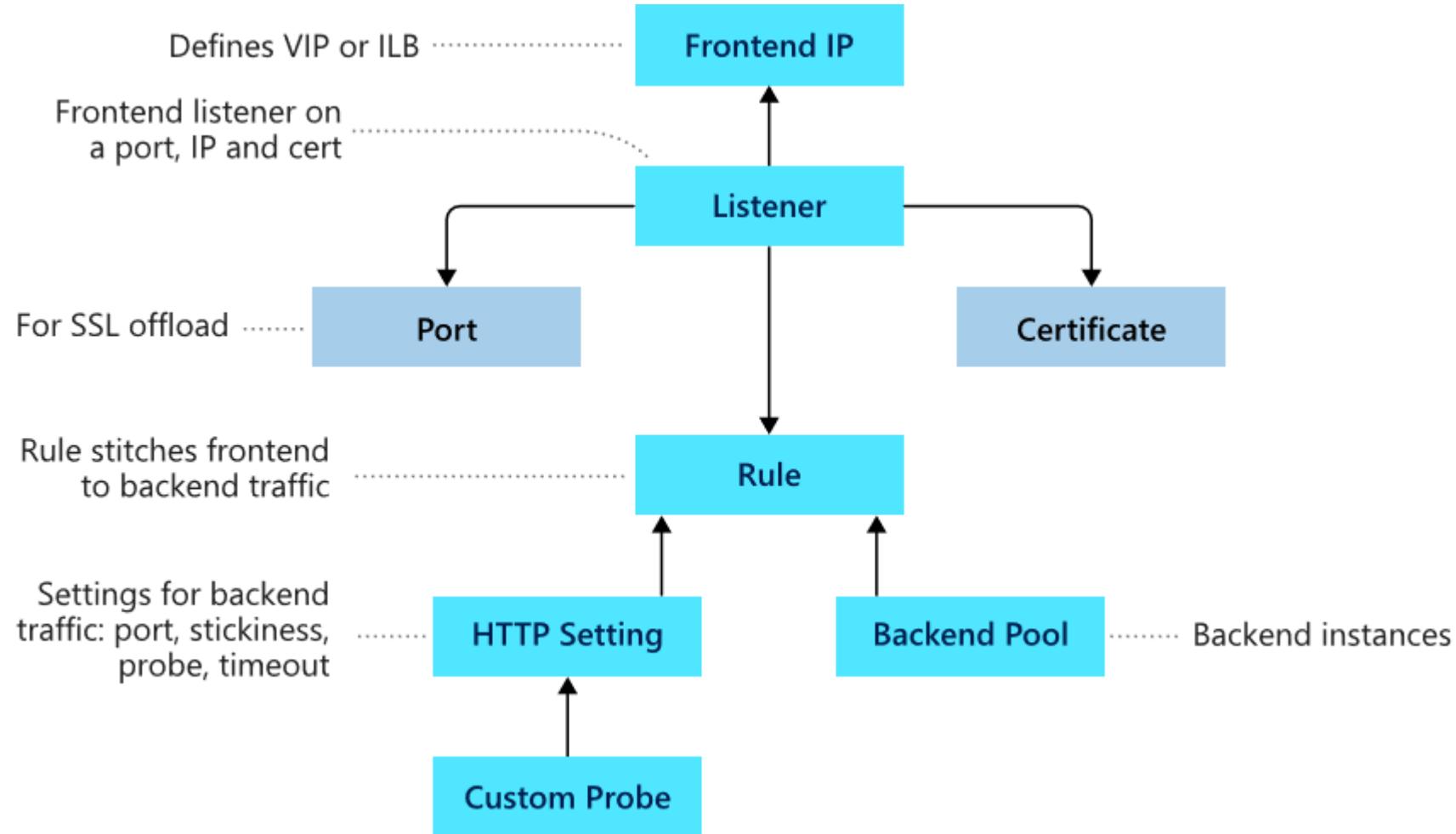


Multiple-site routing



Application Gateway Components

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



Azure Traffic Manager

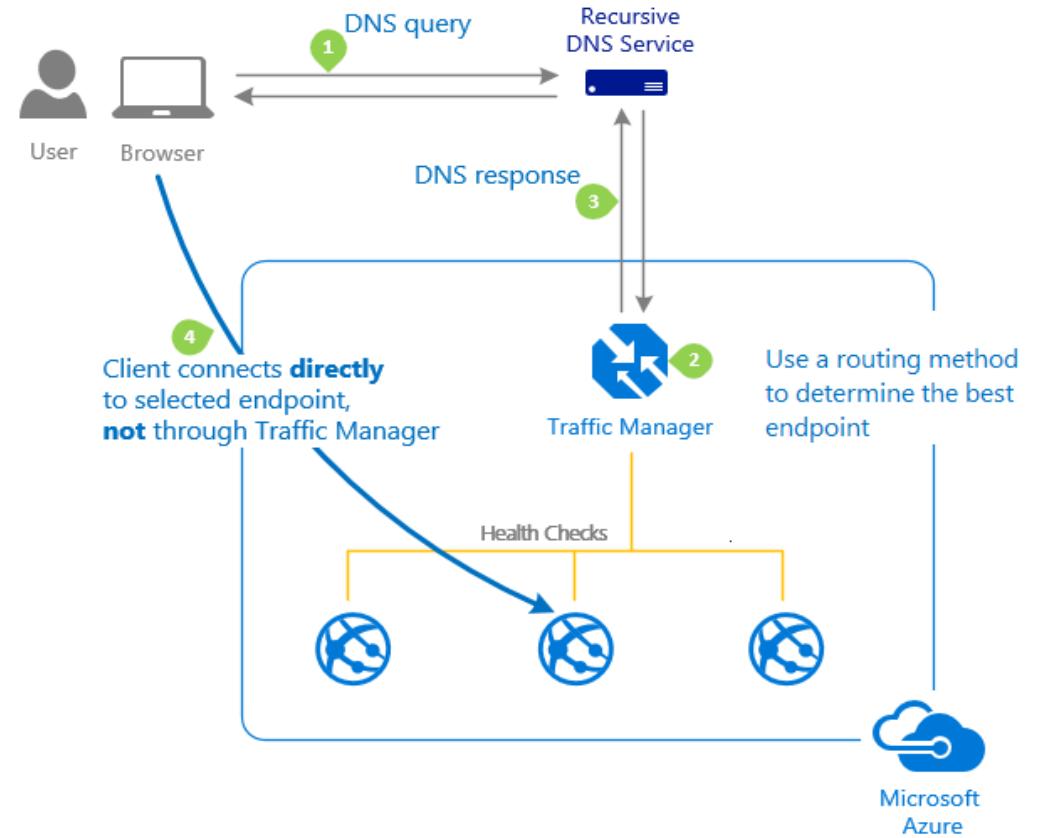


Traffic Manager Overview

- Azure Traffic Manager
- Traffic Manager Routing Methods
- Distributing Network Traffic

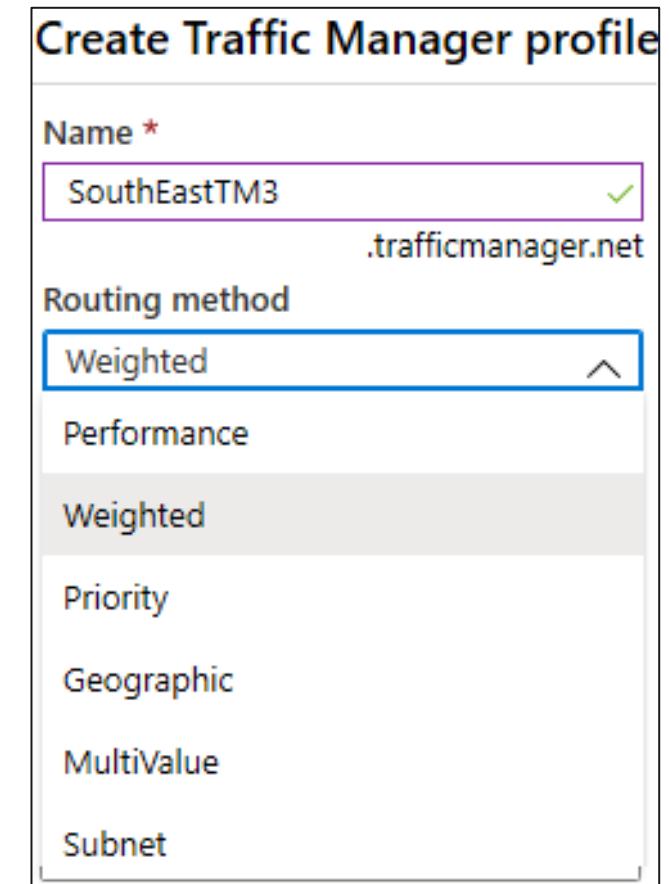
Azure Traffic Manager

- Allows you to control distribution of user traffic to service endpoints around the world
- Uses DNS to direct end-user requests to the most appropriate endpoint
- Selects an endpoint based on the configuring traffic-routing method
- Provides endpoint health checks and automatic endpoint failover



Traffic Manager Routing Methods

- Priority routing routes traffic to a prioritized list of service endpoints
- Performance routing Routes traffic to the location closest to the user
- Geographic routing routes traffic to a set of geographic locations
- Weighted routing distributes traffic evenly using a pre-defined weighting
- MultiValue routing distributes traffic only to IPv4 and IPv6 endpoints
- Subnet routing distributes traffic based on source IP ranges



Distributing Network Traffic

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport Layer (level 4)	Application Layer (level 7)	DNS Resolver
Protocols	Any TCP or UDP Protocol	HTTP, HTTPS, HTTP/2, & WebSockets	DNS Resolution
Backends or Endpoints	Azure Virtual Machines, and Azure Virtual Machine Scale Sets	Azure Virtual Machines, Azure Virtual Machine Scale Sets, Azure App Services, IP Addresses, and Hostnames	Azure Cloud Services, Azure App Services, Azure App Service Slots, and Public IP Addresses
Network Connectivity	External and Internal	External and Internal	External

- Azure has several options to distribute network traffic
- They can each be used in isolation or in combination

Module 06 Lab and Review



Lab 06 – Implement Traffic Management

Scenario

You are tasked with implementing a hub spoke topology for network traffic. The topology should include an Azure Load Balancer and Azure Application Gateway.

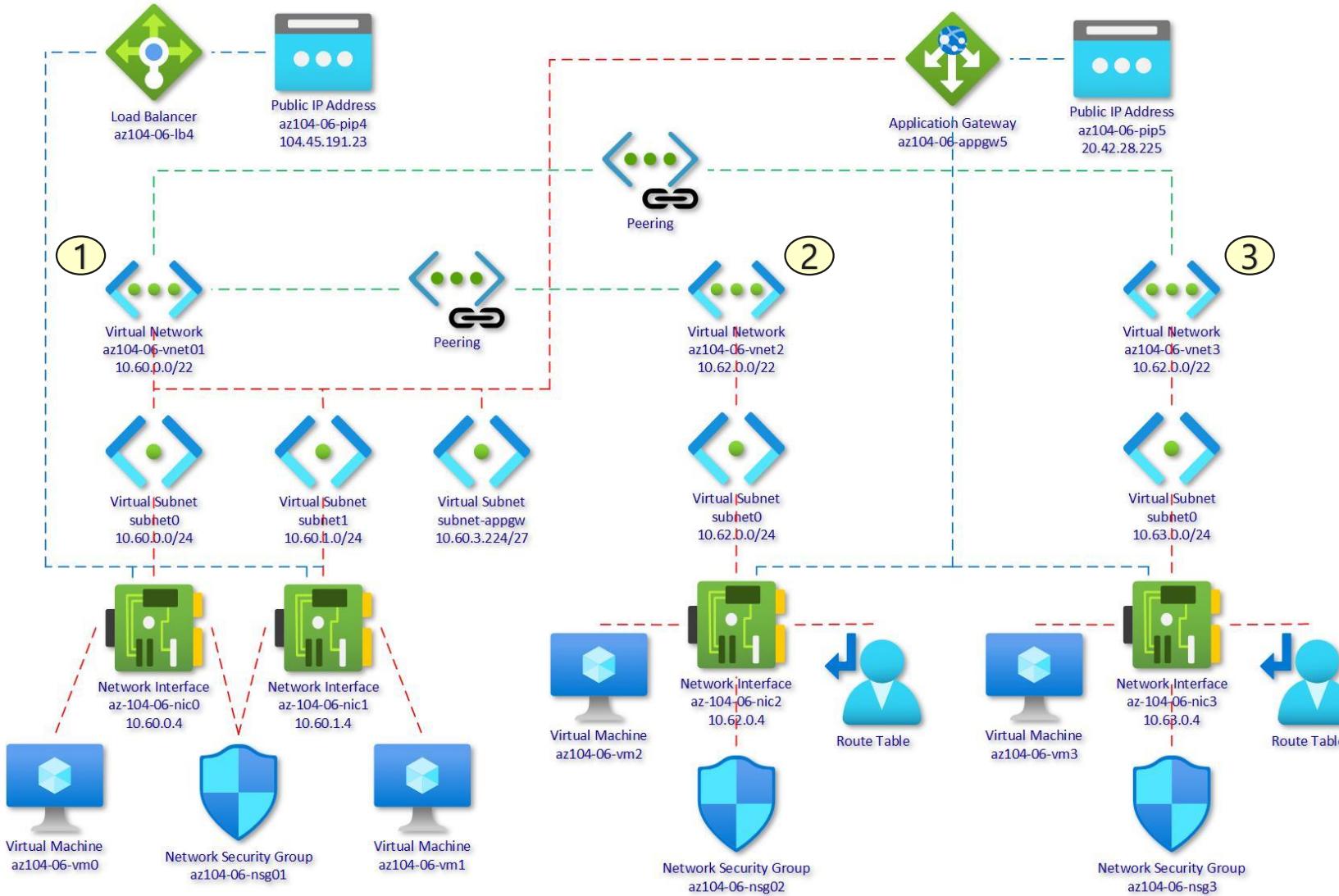
Objectives

- Task 1: Provision the lab environment
- Task 2: Configure the hub and spoke network topology
- Task 3: Test transitivity of virtual network peering
- Task 4: Configure routing in the hub and spoke topology
- Task 5: Implement Azure Load Balancer
- Task 6: Implement Azure Application Gateway

Next slide for
an architecture diagram



Lab 06 – Architecture Diagram





AZ-104T00A

Module 07:

Azure Storage



Module Overview

- Storage Accounts
- Blob Storage
- Storage Security
- Azure Files and File Sync
- Managing Storage

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
- Manage data with multiple storage accounts
- Three categories of Azure storage:
 - Storage for virtual machines – Disks and File Shares
 - Unstructured data – Blobs and Data Lake Store
 - Structured data - Tables, Cosmos DB, and Azure SQL DB
- Standard storage backed by magnetic drives (HDD) is lowest cost
- Premium storage backed by solid state drives (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



Containers

Scalable, cost-effective storage for unstructured data

[Learn more](#)



File shares

Serverless SMB file shares

[Learn more](#)



Tables

Tabular data storage

[Learn more](#)



Queues

Effectively scale apps according to traffic

[Learn more](#)

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

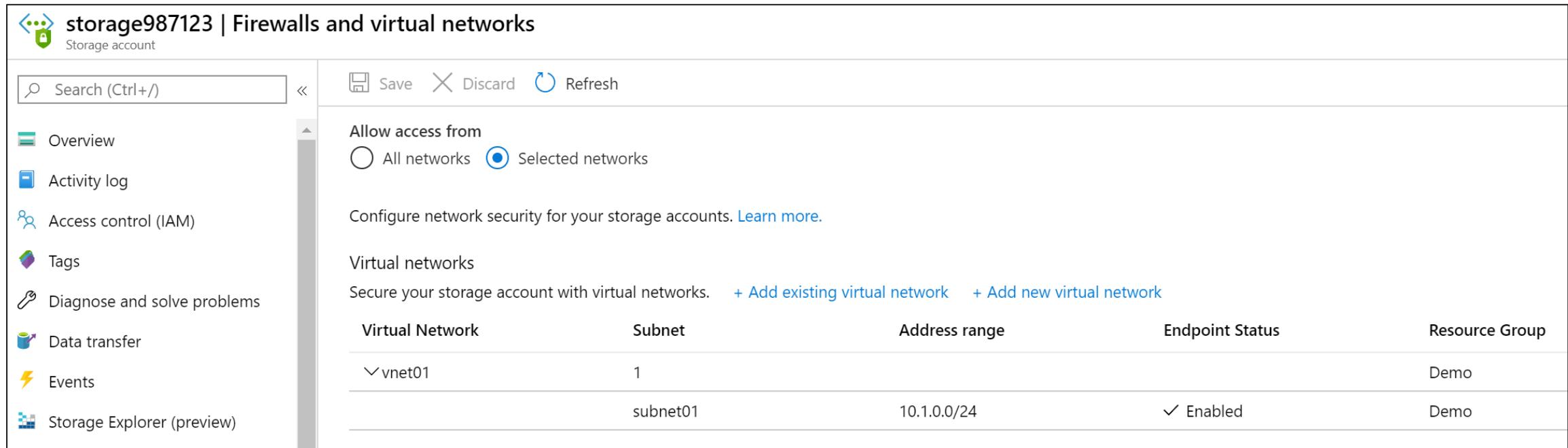
Data Replication Options	Description
Locally redundant storage (LRS)	Data is replicated three time within a single facility in a single region.
Zone-redundant storage (ZRS)	Data is replicated three times across two to three facilities, either within a single region or across two regions.
Geo-redundant storage (GRS)	Data is replicated three times within the primary region and replicated three times to the regions pair.

Accessing Storage

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

- Every object has a unique URL address
- The storage account name forms the subdomain of that address
- The subdomain and domain name forms an *endpoint*
 - **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



The screenshot shows the 'Firewalls and virtual networks' section of the Azure Storage account settings for 'storage987123'. On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data transfer, Events, and Storage Explorer (preview). The main area has a search bar and buttons for Save, Discard, and Refresh. It displays the 'Allow access from' section with 'Selected networks' selected. Below that is a note about configuring network security. Under 'Virtual networks', it says 'Secure your storage account with virtual networks.' followed by '+ Add existing virtual network' and '+ Add new virtual network'. A table lists the configured virtual network and subnet:

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group
vnet01	1			Demo
	subnet01	10.1.0.0/24	✓ Enabled	Demo

- 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

Blob Storage

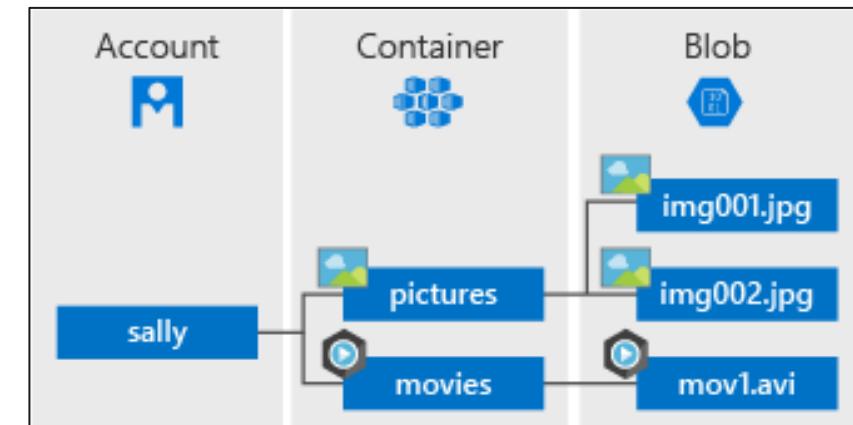


Blob Storage Overview

- Blob Storage
- Blob Containers
- Blob Access Tiers
- Blob Lifecycle Management
- Uploading Blobs
- Storage Pricing

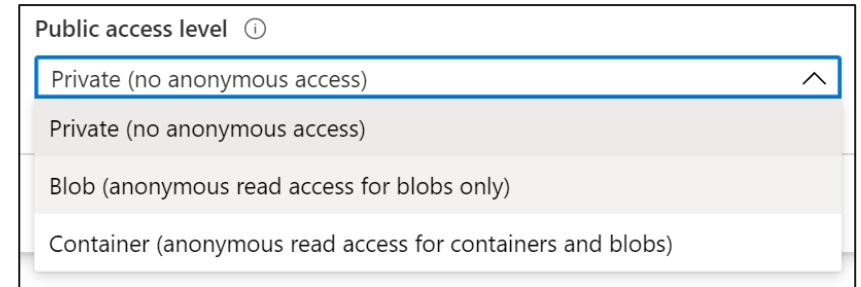
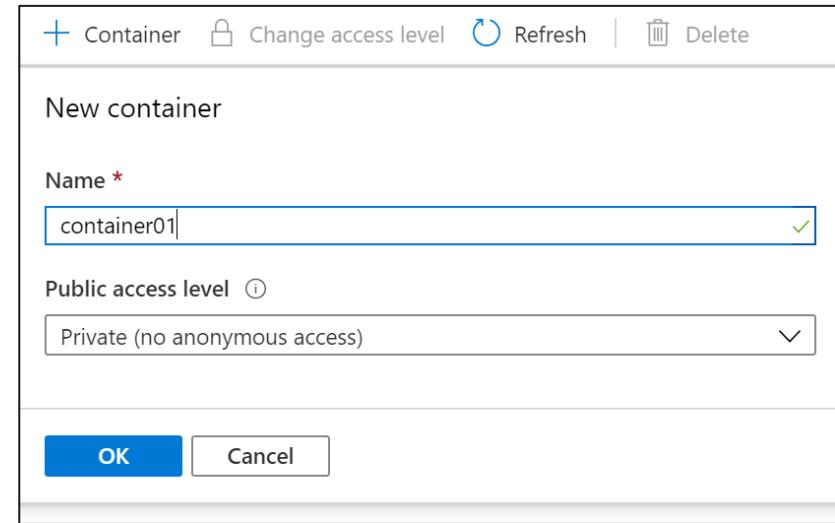
Blob Storage

- 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



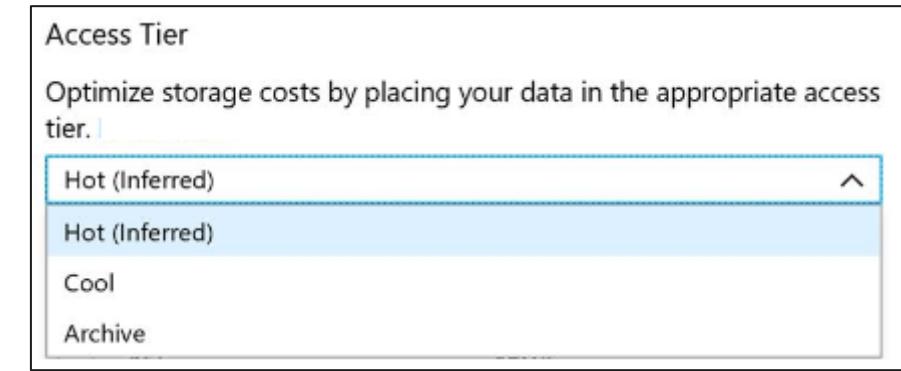
Blob Containers

- 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

Blob Lifecycle Management allows for:

- 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

Rule name *

 ✓

Blobs

Move blob to cool storage

Days after last modification ✓

Move blob to archive storage

Days after last modification ✓

Delete blob

Days after last modification ✓

Snapshots

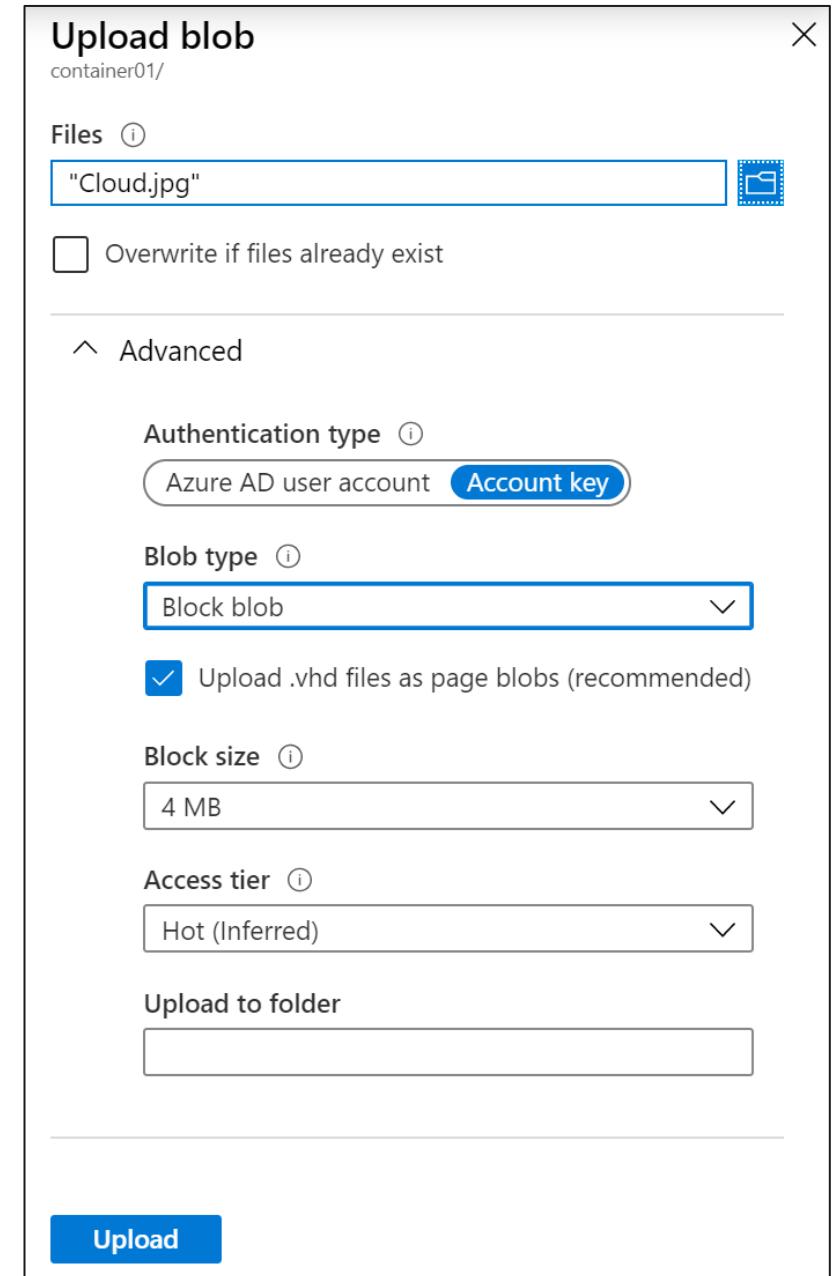
Delete snapshot

Days after blob is created ✓

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

Block Blobs	Files
<p>Scalable object storage for documents, videos, pictures, and unstructured text or binary data. Choose from Hot, Cool, or Archive tiers.</p> <p>Prices for locally redundant storage (LRS) Archive Block Blob start from:</p> <p>\$0.002/GB per month</p> <p>See Pricing ></p>	<p>Fully managed file shares in the cloud, accessible via standard Server Message Block (SMB) protocol. Enables sharing files between applications using Windows APIs or REST API.</p> <p>Prices for LRS File storage start from:</p> <p>\$0.06/GB per month</p> <p>See Pricing ></p>

Storage Security



Storage Security Overview

- Storage Security
- Shared Access Signatures
- URI and SAS Parameters
- Storage Service Encryption
- Customer Managed Keys
- 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

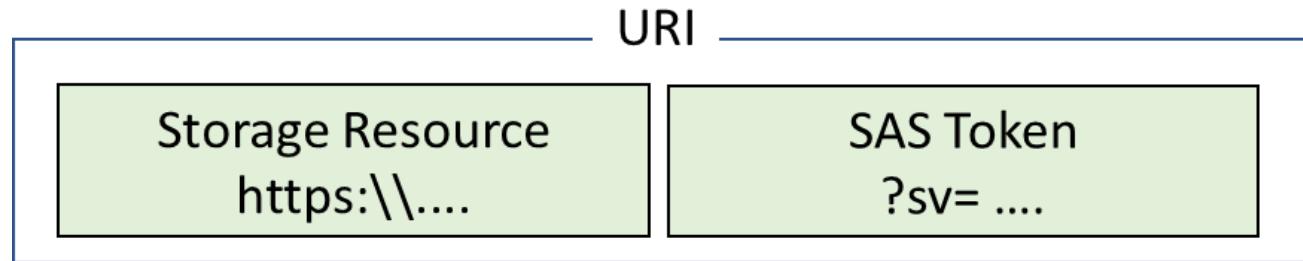
- Provides delegated access to resources
- Grants access to clients without sharing your storage account keys
- The account SAS delegates access to resources in one or more of the storage services
- The service SAS delegates access to a resource in just one of the storage services

The screenshot shows the configuration options for generating a Shared Access Signature (SAS). The interface includes:

- Permissions:** Set to "Read".
- Start and expiry date/time:** Both set to "2019-02-27 7:32:03 AM" and "2019-02-27 3:32:03 PM" in the "(UTC-08:00) --- Current Time Zone ---" time zone.
- Allowed IP addresses:** A placeholder text area with the example "168.1.5.65 or 168.1.5.65-168.1.5.70".
- Allowed protocols:** Radio buttons for "HTTPS" (selected) and "HTTP".
- Signing key:** A dropdown menu showing "Key 1".
- Generate blob SAS token and URL:** A blue button at the bottom.

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=j0qABJZHfUVeBQ3yVn7kWiCKl00sxCiK1rzEchfAz8U%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

Encryption

 Save  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data in the storage account is encrypted using Microsoft Managed Keys. You may choose to bring your own key.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn More about Azure Storage Encryption](#)

Encryption type

Microsoft Managed Keys

Customer Managed Keys

✓ 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

Encryption type

Microsoft Managed Keys
 Customer Managed Keys

i The storage account named 'storage987123' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more about customer managed keys](#)

Encryption key

Enter key URI
 Select from Key vault

Key vault and key *

Key vault: keyvault987123
Key: storagekey
[Select a key vault and key](#)

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

Azure Files and File Sync



Azure Files and File Sync Overview

- Files vs Blobs
- Managing File Shares
- File Share Snapshots
- Azure File Sync
- Azure File Sync Components
- 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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

Windows Linux macOS

Drive letter

z

To connect to this Azure file share from Windows, run these PowerShell commands from a normal (not elevated) PowerShell terminal:

```
$connectTestResult = Test-NetConnection -  
ComputerName storage987123.file.core.windows.net -  
Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # Save the password so the drive will persist on reboot  
    cmd.exe /C "cmdkey  
/add:"storage987123.file.core.windows.net"
```



This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), Azure [Site-to-Site \(S2S\) VPN](#), or [ExpressRoute](#) to tunnel SMB traffic to your Azure file share over a different port.

File Share Snapshots

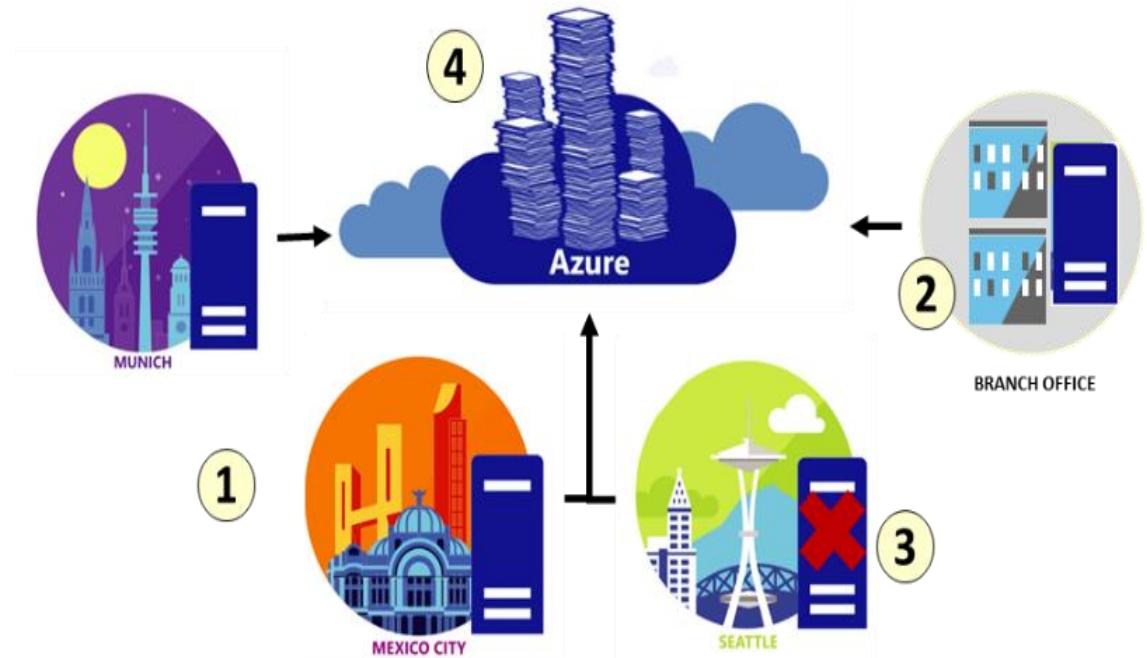
Name	Date created	Initiator
<input type="checkbox"/> 2020-03-12T00:58:38.0000000Z	3/11/2020, 8:58:38 PM	-

- 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

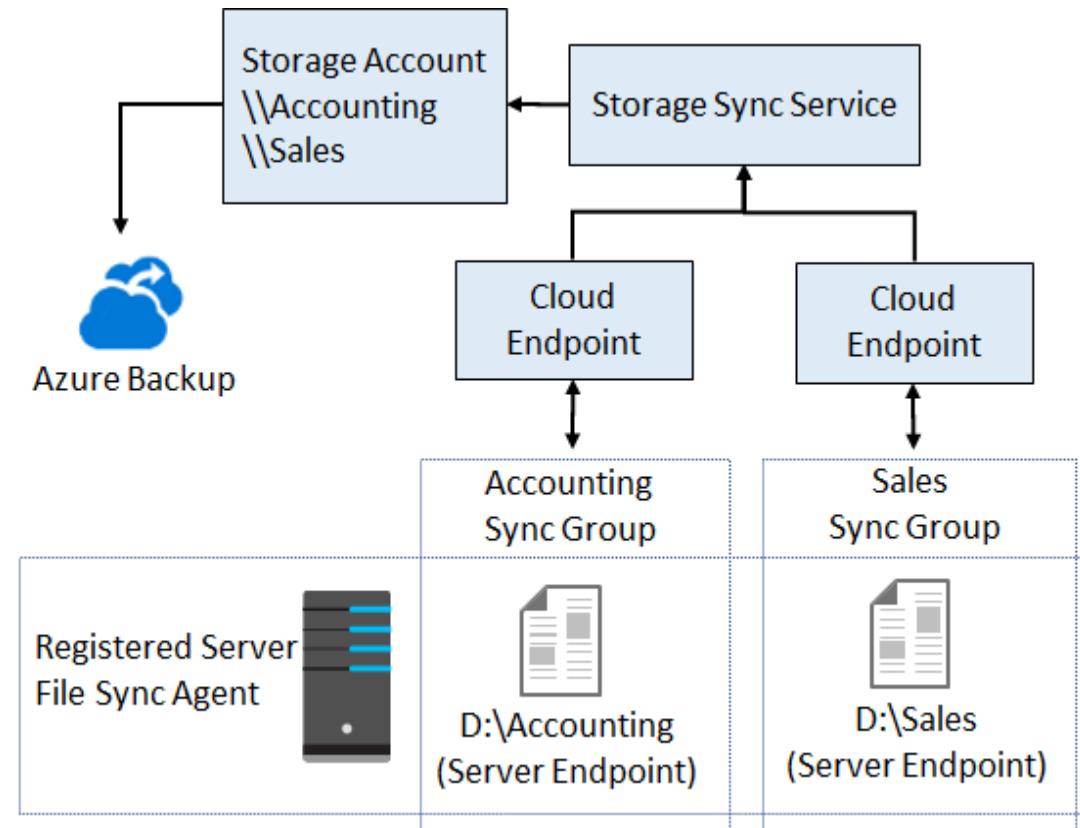
Centralize file shares in Azure Files

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

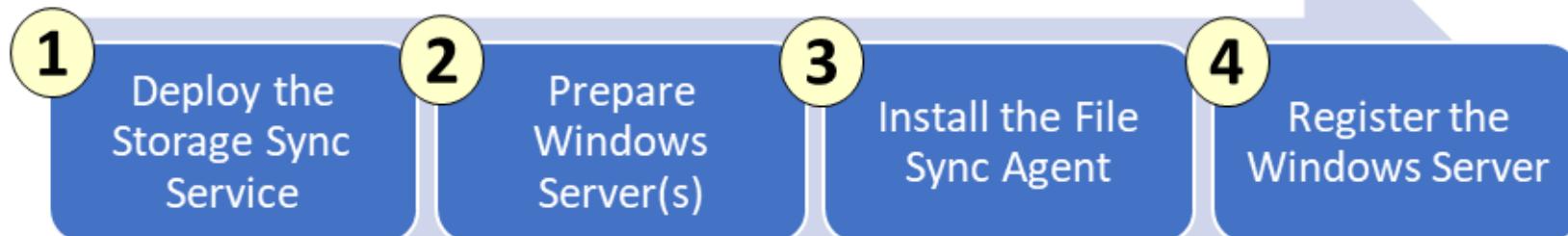


File Sync Components

- 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



Home > Deploy Storage Sync

Deploy Storage Sync

* Name: StorageSync1

* Subscription: Visual Studio Enterprise

* Resource group: ASH

Create new

* Location: South Central US

Create **Automation options**

Microsoft Azure File Sync - Server Registration

Choose a Storage Sync Service

Azure Subscription:

Resource Group:

Storage Sync Service:

Register

Managing Storage

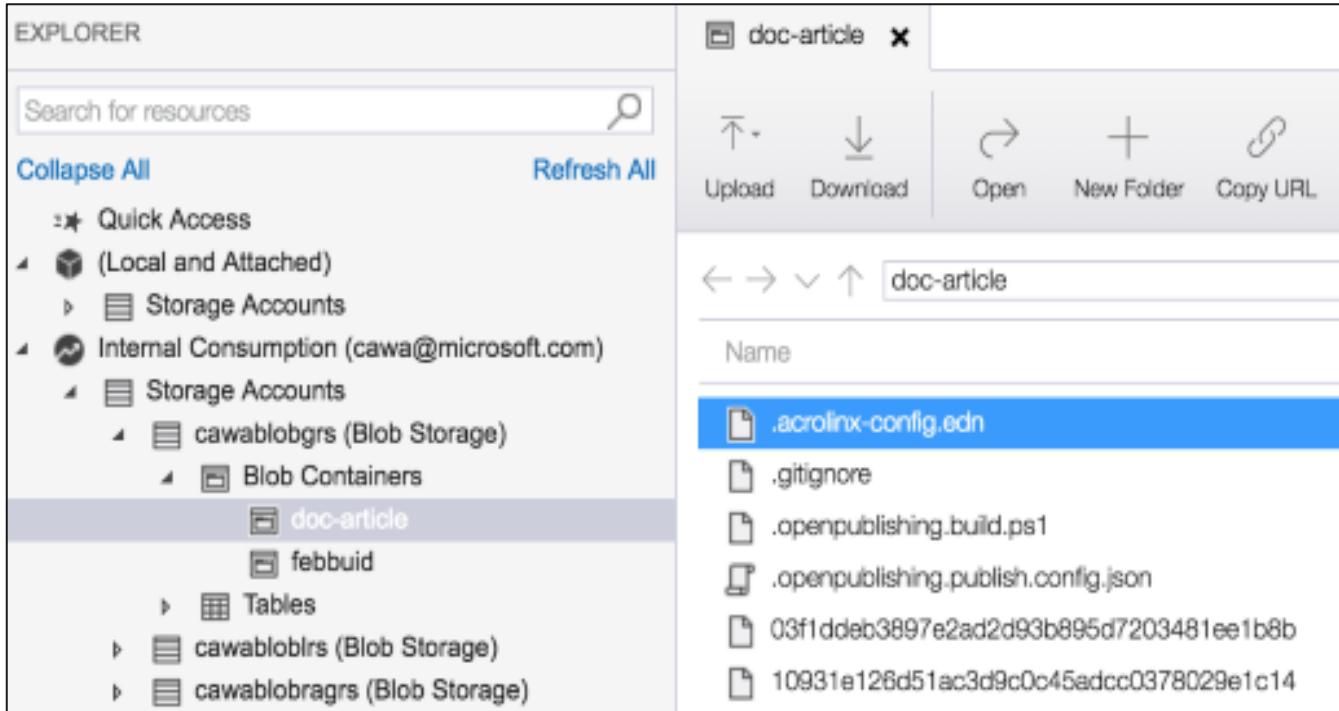


Managing Storage Overview

- Storage Explorer
- Import and Export Service
- Data Box
- AzCopy
- Data Transfer Tool Selection

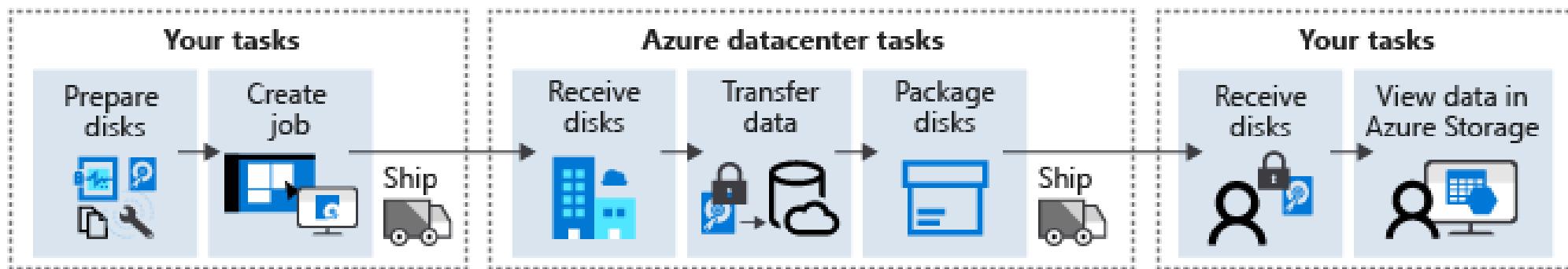
Storage Explorer

- 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

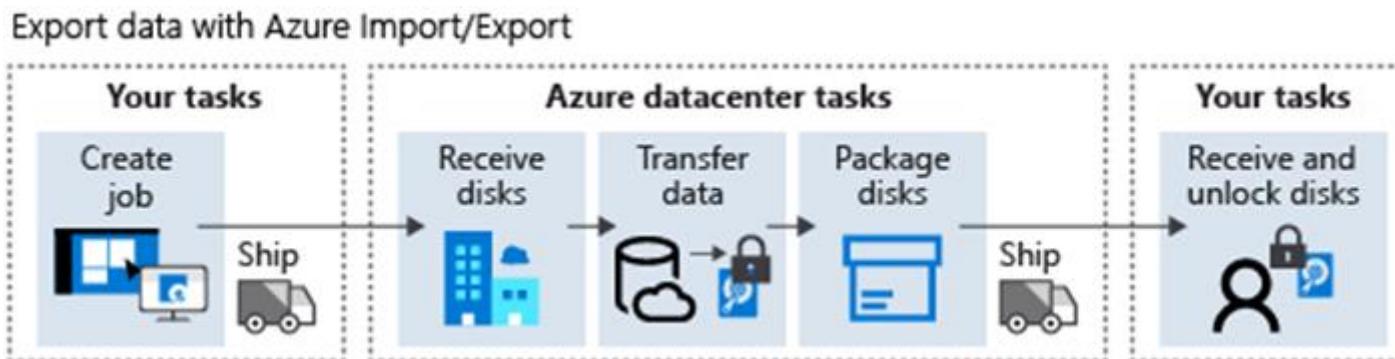


Import and Export Service

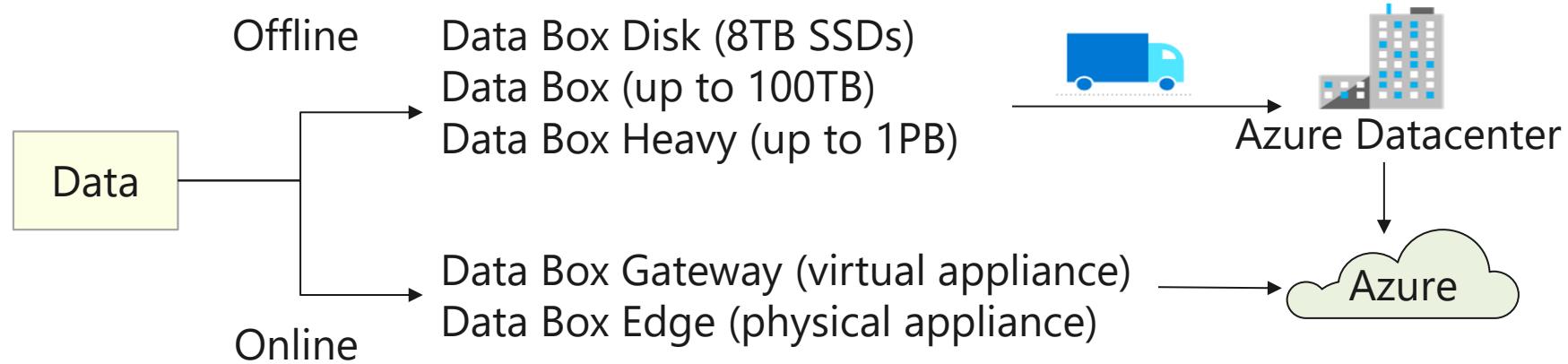
- Import jobs move large amounts of data to Azure blob storage or files



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



Data Box



- Easy, secure, fast large volume data transfer
- **Offline** usage - one-time migration, incremental transfer, periodic updates
- **Online** usage – cloud archival, data aggregation, integration with on-premises workloads, pre-process data (Edge), inference Azure Machine Learning (Edge)

AzCopy

```
azcopy copy /Source:<source> /Dest:<destination> [Options]
```

- Command-line utility
- Available on Windows, Linux, and MacOS
- Designed for copying data to and from Azure Blob, File, and Table storage
- Authentication options include Active Directory or SAS token
- Example 1: Copy a Blob storage account to another account
- Example 2: List/Remove files and blobs (wildcard support)

Data Transfer Tool Selection

Dataset	Network bandwidth	Solution to use
Large dataset	Low-bandwidth network or direct connectivity to on-premises storage is limited by organization policies	Azure Import/Export for export; Data Box Disk or Data Box for import where supported; otherwise use Azure Import/Export
Large dataset	High-bandwidth network: 1 gigabit per second (Gbps) - 100 Gbps	AzCopy for online transfers; or to import data, Azure Data Box Edge, or Azure Data Box Gateway
Large dataset	Moderate-bandwidth network: 100 megabits per second (Mbps) - 1 Gbps	Azure Import/Export for export or Azure Data Box family for import where supported
Small dataset: a few GBs to a few TBs	Low to moderate-bandwidth network: up to 1 Gbps	If transferring only a few files, use Azure Storage Explorer, Azure portal, AzCopy, or AZ CLI

Module 07 Labs and Review





AZ-104T00A

Module 08:

Azure Virtual Machines



Module Overview

- Virtual Machine Planning
- Creating Virtual Machines
- Virtual Machine Availability
- Virtual Machine Extensions

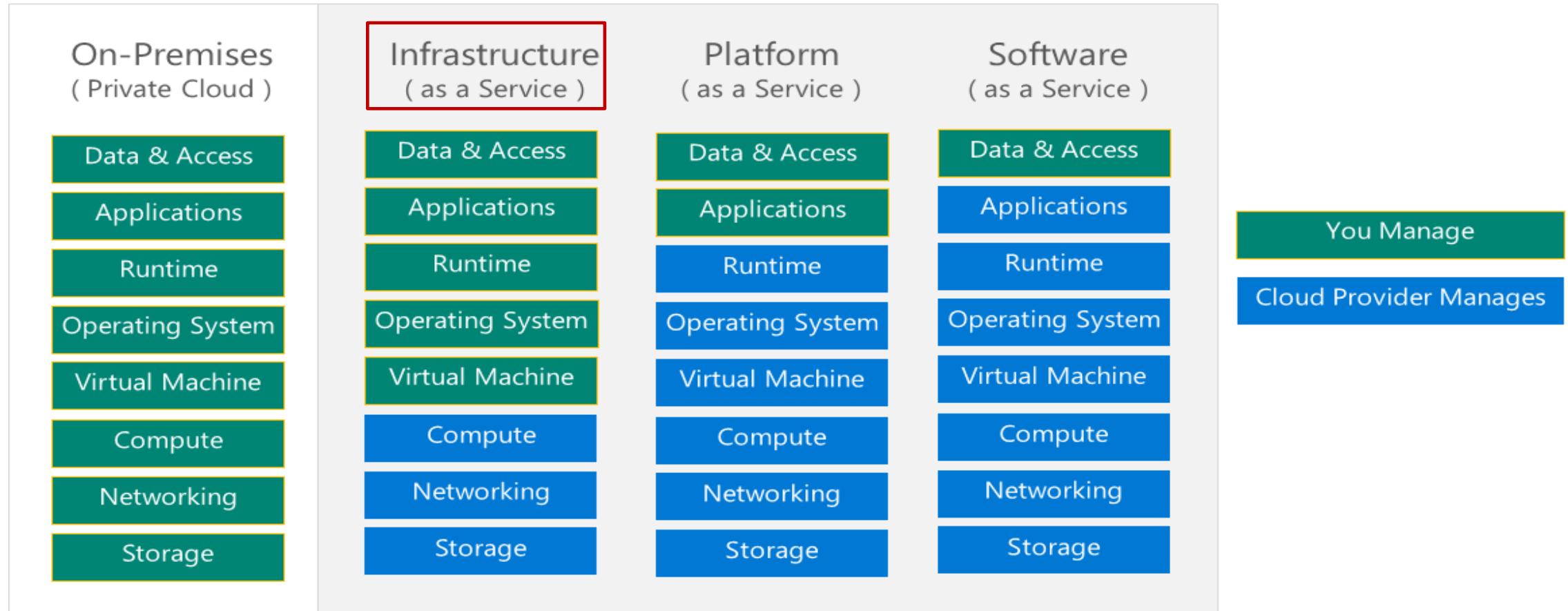
Virtual Machine Planning



Virtual Machine Planning Overview

- IaaS Cloud Services
- Planning Checklist
- Location and Pricing
- Virtual Machine Sizing
- Virtual Machine Disks
- Storage Options
- Supported Operating Systems
- 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
- Name the VM
- Decide the location for the VM
- Determine the size of the VM
- Understand the pricing model
- Consider storage for the VM
- Select an operating system

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)



55+ Azure regions
Available in 140 countries

Virtual Machine Sizing

VM Type	Sizes	Purpose
General Purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute Optimized	Fsv2	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory Optimized	Esv3, Ev3, Easv4, Eav4, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage Optimized	Lsv2	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NC, NCv2, NCv3, ND, NDv2 (Preview), NV, NVv3, NVv4 (Preview)	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High Performance Compute	HB, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

Virtual Machine Disks

NAME	SIZE	STORAGE ACCOUNT...	ENCRYPTION	HOST CACHING
UbuntuServer_OsDisk_1_	30 GiB	Standard_LRS	Not enabled	Read/write

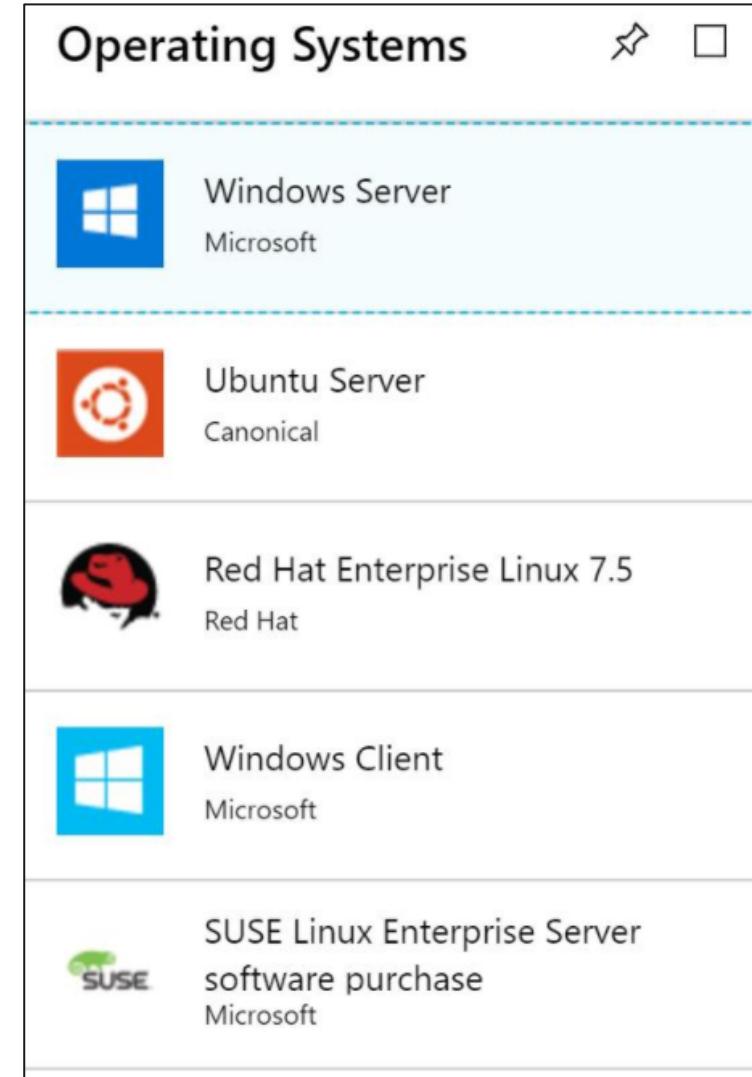
- Operating System Disks are SATA drives, labeled as C:
- Temporary Disks provides short term storage
- Data Disks are SCSI drives and depend on your virtual machine type

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)

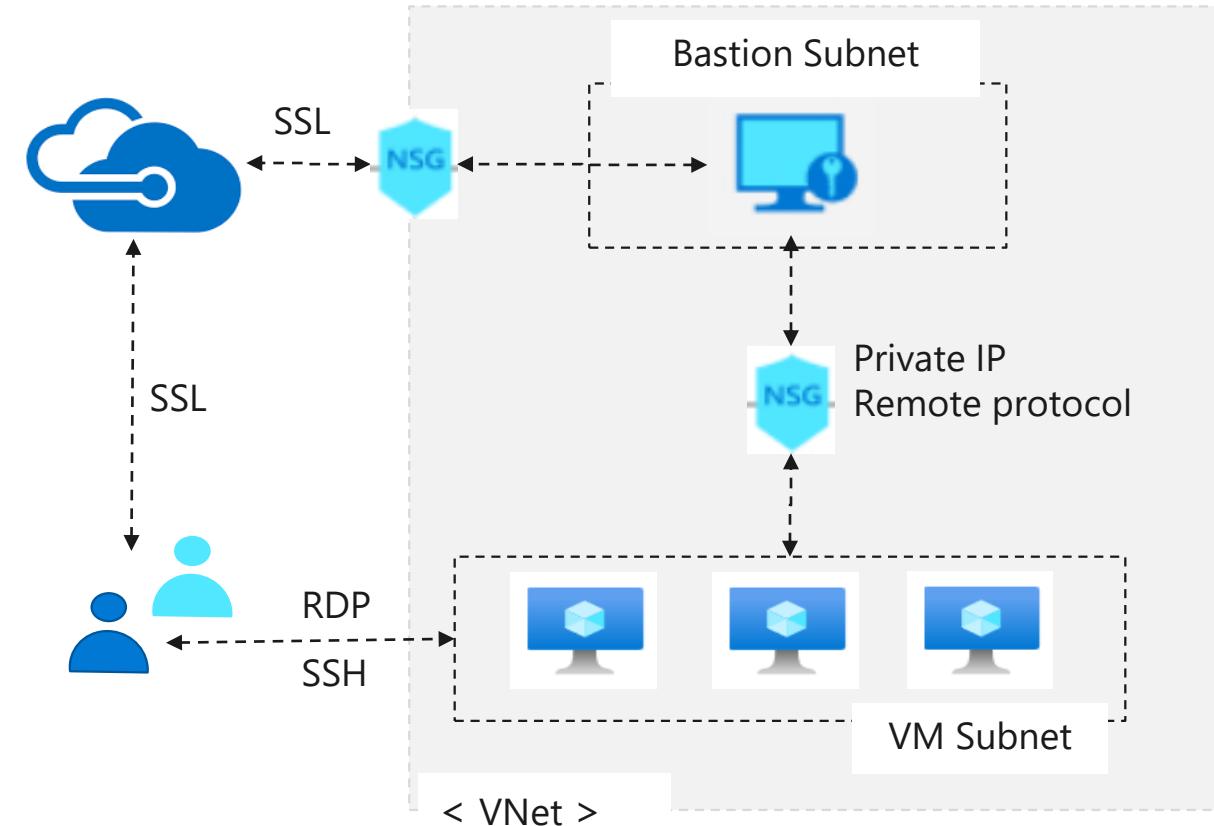
Supported Operating Systems

- 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



Creating Virtual Machines

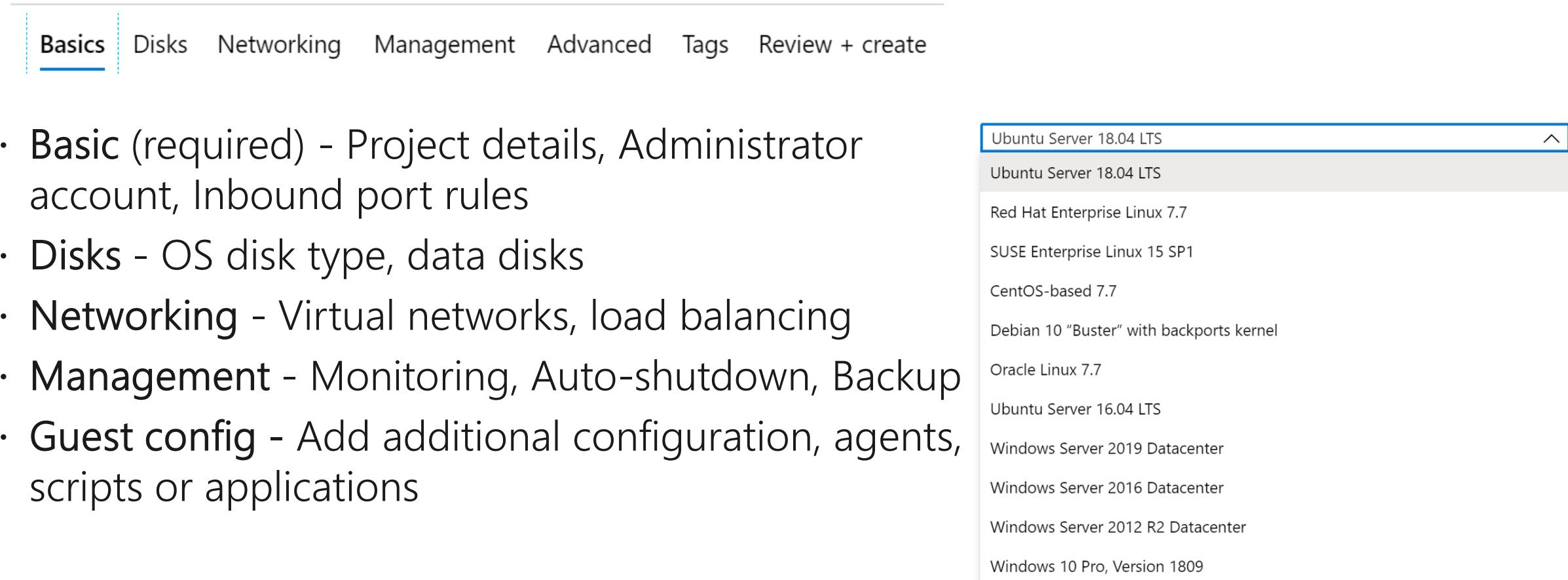


Creating Virtual Machines Overview

- Creating Virtual Machines in the Portal
- Windows Virtual Machines
- Windows VM Connections
- Linux Virtual Machines
- Linux VM Connections

Creating Virtual Machines in the Portal

Create a virtual machine



The screenshot shows a user interface for creating a virtual machine. At the top, there is a navigation bar with tabs: Basics (which is underlined in blue), Disks, Networking, Management, Advanced, Tags, and Review + create. Below the navigation bar, there is a list of steps or sections:

- 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
- Guest config - Add additional configuration, agents, scripts or applications

On the right side of the interface, there is a dropdown menu showing a list of operating system options:

- Ubuntu Server 18.04 LTS
- Ubuntu Server 18.04 LTS
- Red Hat Enterprise Linux 7.7
- SUSE Enterprise Linux 15 SP1
- CentOS-based 7.7
- Debian 10 "Buster" with backports kernel
- Oracle Linux 7.7
- Ubuntu Server 16.04 LTS
- Windows Server 2019 Datacenter
- Windows Server 2016 Datacenter
- Windows Server 2012 R2 Datacenter
- Windows 10 Pro, Version 1809

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



Debian Linux
By credativ
Debian GNU/Linux for Microsoft Azure provided by credativ.

Software plans start at Free

[Get it now](#)



Clear Linux OS
By Clear Linux Project
A reference Linux distribution optimized for Intel Architecture.

[Bring your own license](#)

[Get it now](#)



SUSE Linux Enterprise Server
By SUSE
SUSE Linux Enterprise Server

Software plans start at Free

[Get it now](#)

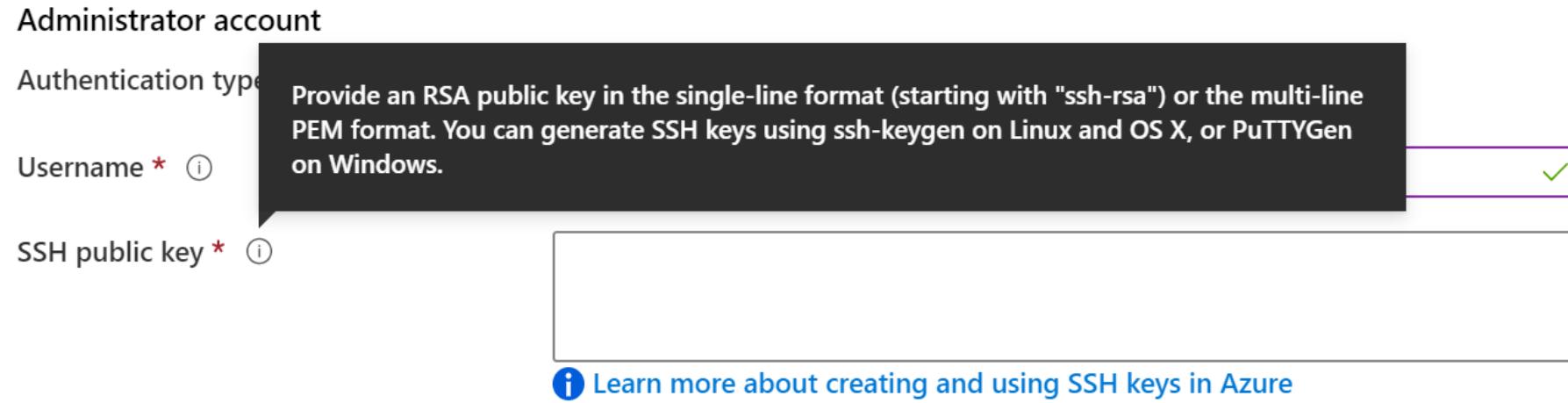


Red Hat Enterprise Linux 7.4
By Red Hat
Red Hat Enterprise Linux 7 is the world's leading enterprise Linux platform built to meet the needs of toda...

[Get it now](#)

- 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

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

Instance details

Name * ⓘ avset01

Region * ⓘ (US) East US

Fault domains ⓘ 2

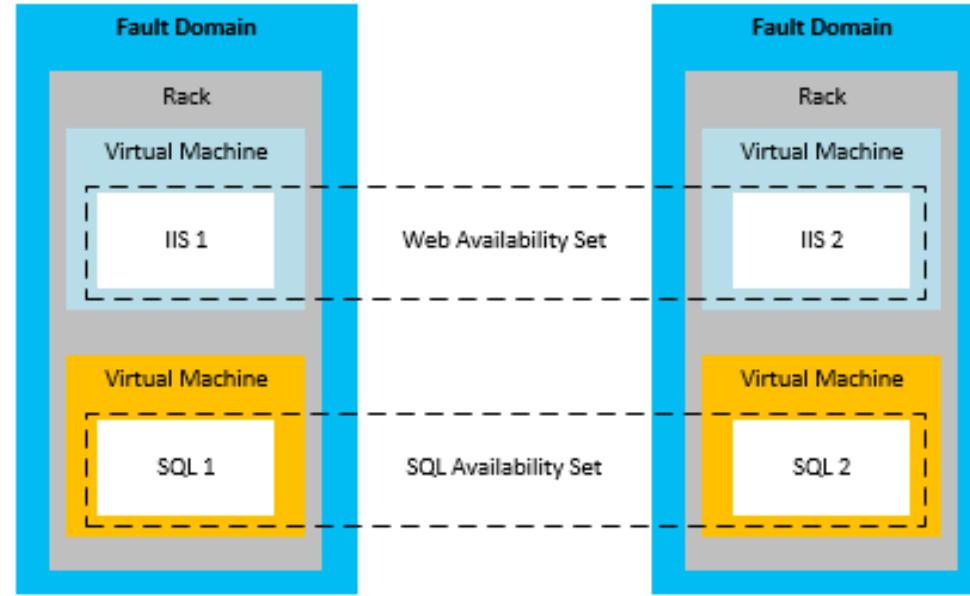
Update domains ⓘ 5

Use managed disks ⓘ No (Classic) Yes (Aligned)

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

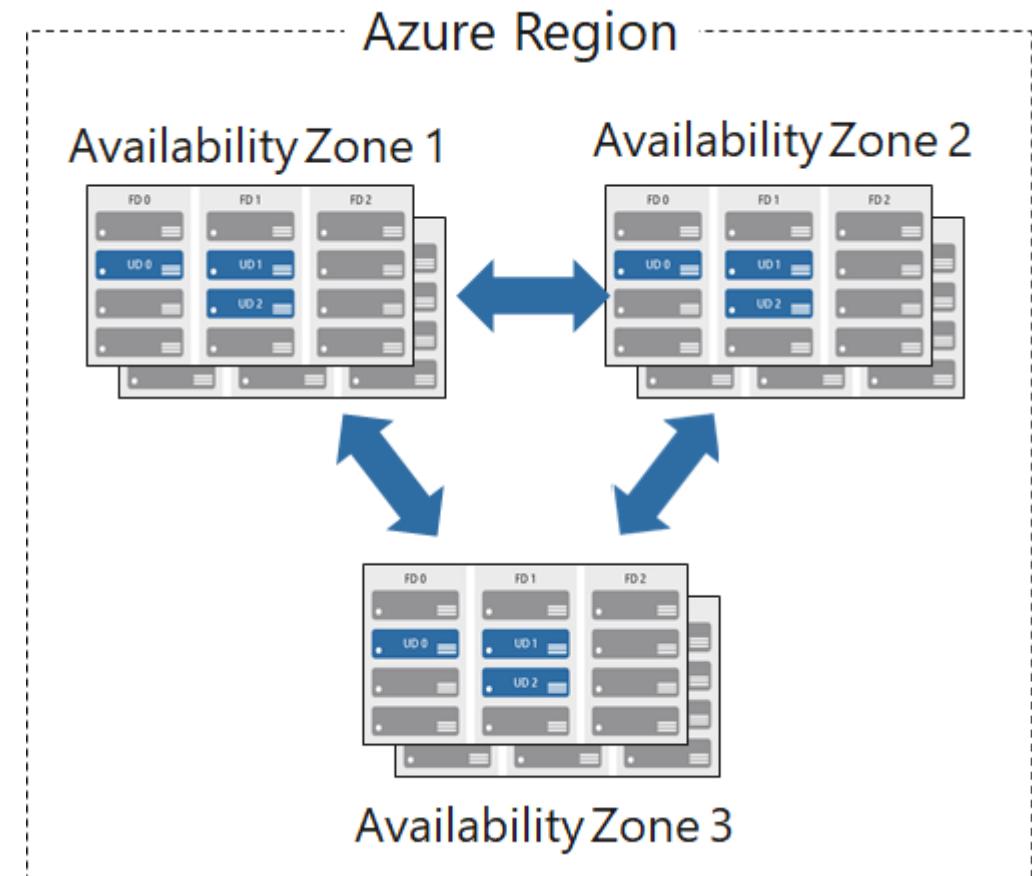
Update and Fault Domains



- 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

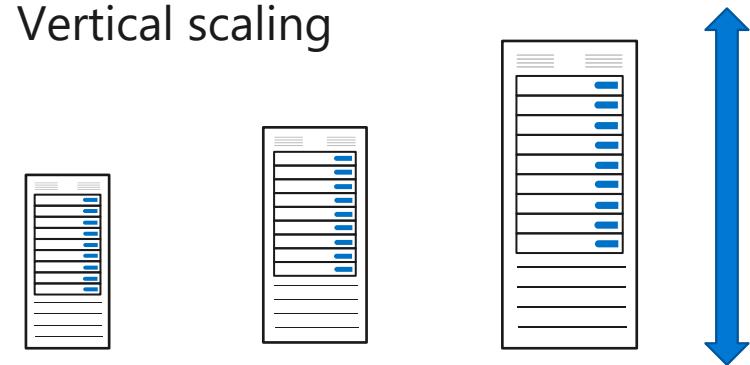
- Unique physical locations in a region
- Includes datacenters with independent power, cooling, and networking
- Protects from datacenter failures
- Combines update and fault domains
- Provides 99.99% SLA



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

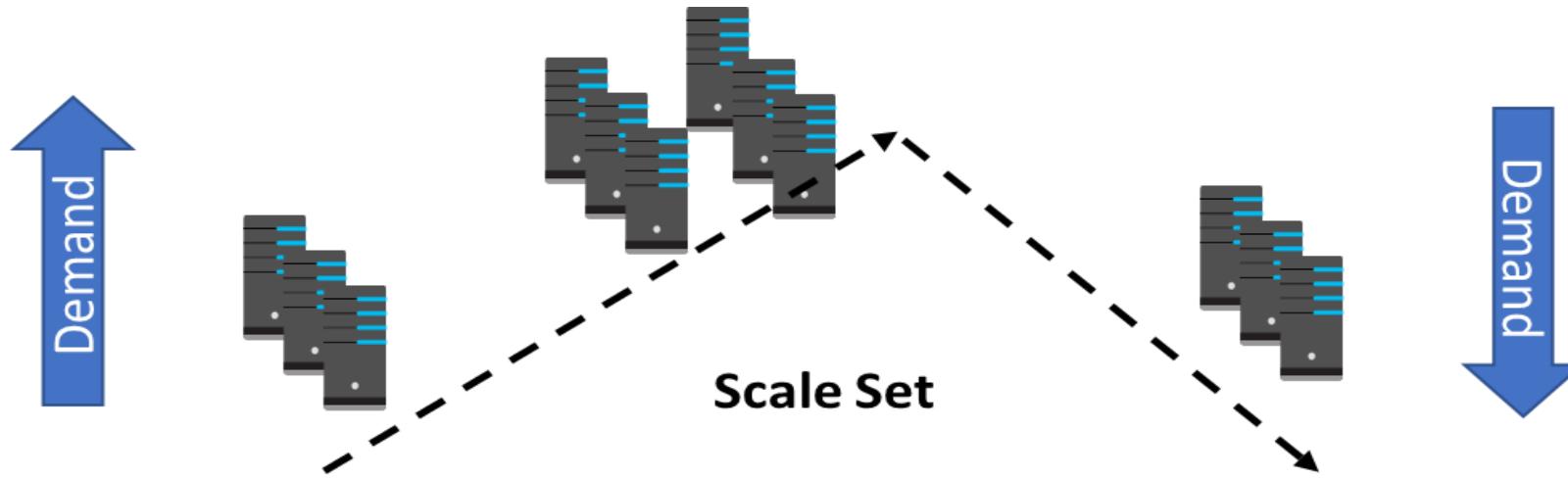
Vertical scaling



Horizontal scaling



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 VMs are removed
- The process can be manual, automated, or a combination of both

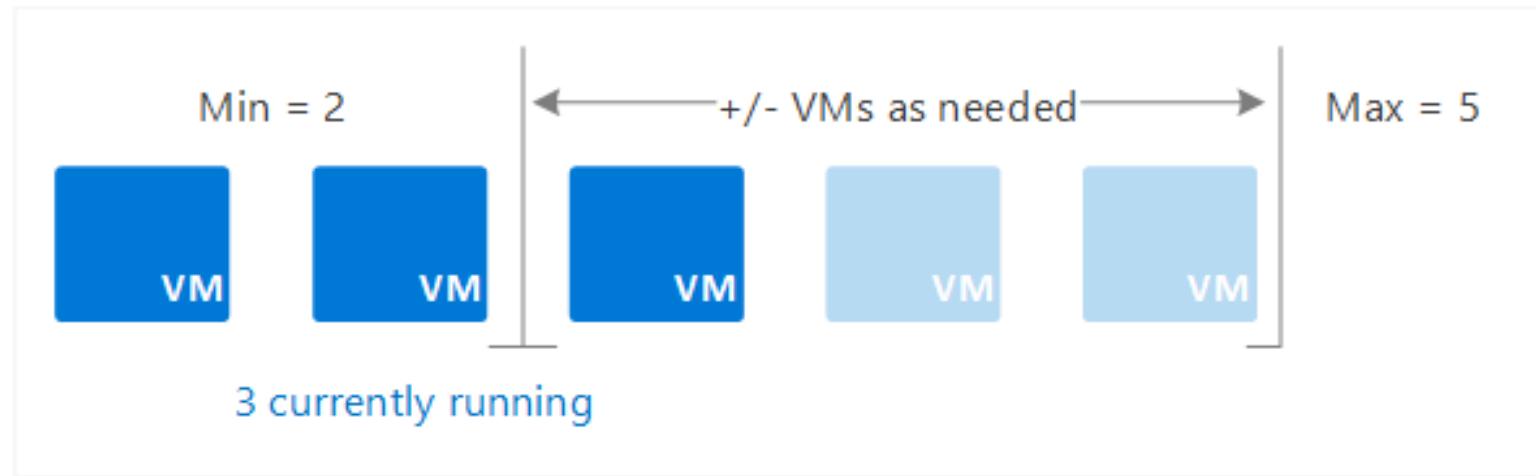
Implementing Scale Sets

- 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

The screenshot shows the configuration options for a new Azure Scale Set. The 'Initial instance count' is set to 2. The 'Size' is selected as 'Standard D2s v3', which provides 2 vcpus and 8 GiB memory at \$85.41/month. The 'Azure Spot instance' option is set to 'No'. The 'Use managed disks' option is set to 'Yes'. Under 'Allocation policy', 'Enable scaling beyond 100 instances' is set to 'No'. The 'Spreading algorithm' is set to 'Fixed spreading (not recommended with zones)'.

Initial instance count *	2
Size *	Standard D2s v3 2 vcpus, 8 GiB memory (\$85.41/month) Change size
Azure Spot instance	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use managed disks	<input type="radio"/> No <input checked="" type="radio"/> Yes
Allocation policy	
Enable scaling beyond 100 instances	<input type="radio"/> No <input checked="" type="radio"/> Yes
Spreading algorithm	<input type="radio"/> Max spreading <input checked="" type="radio"/> Fixed spreading (not recommended with zones)

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

Virtual Machine Extensions

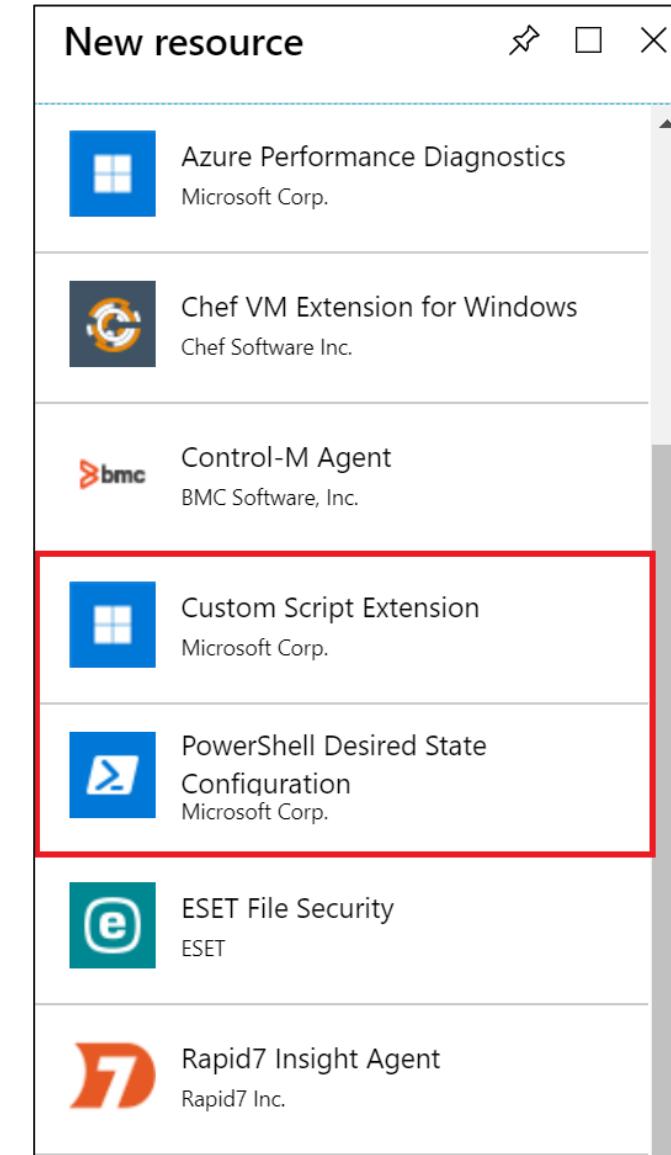


Virtual Machine Extensions Overview

- Virtual Machine Extensions
- Custom Script Extensions
- Desired State Configuration

Virtual Machine Extensions

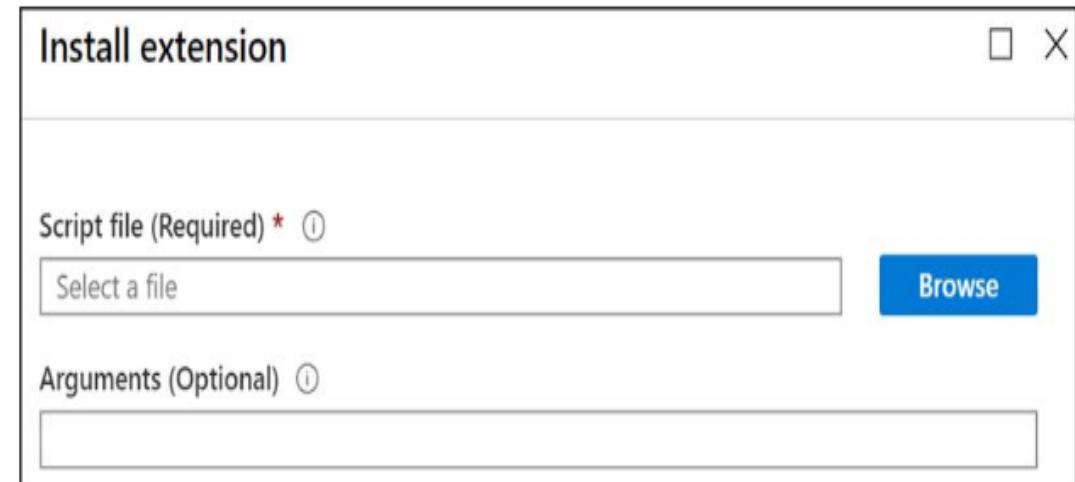
- Extensions are small applications that provide post-deployment VM configuration and automation tasks
- Managed with Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal
- Bundled with a new VM deployment or run against any existing system
- Different for Windows and Linux machines



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



Module 08 Lab and Review



AZ-104T00A

Module 09:

Serverless Computing



Module Overview

- Azure App Service Plans
- Azure App Services
- Container Services
- Azure Kubernetes Service

Azure App Service Plans



Azure App Service Overview

- Azure App Service Plans
- App Service Plan Pricing Tiers
- App Service Plan Scaling
- App Service Plan Scale Out

Azure App Service Plans

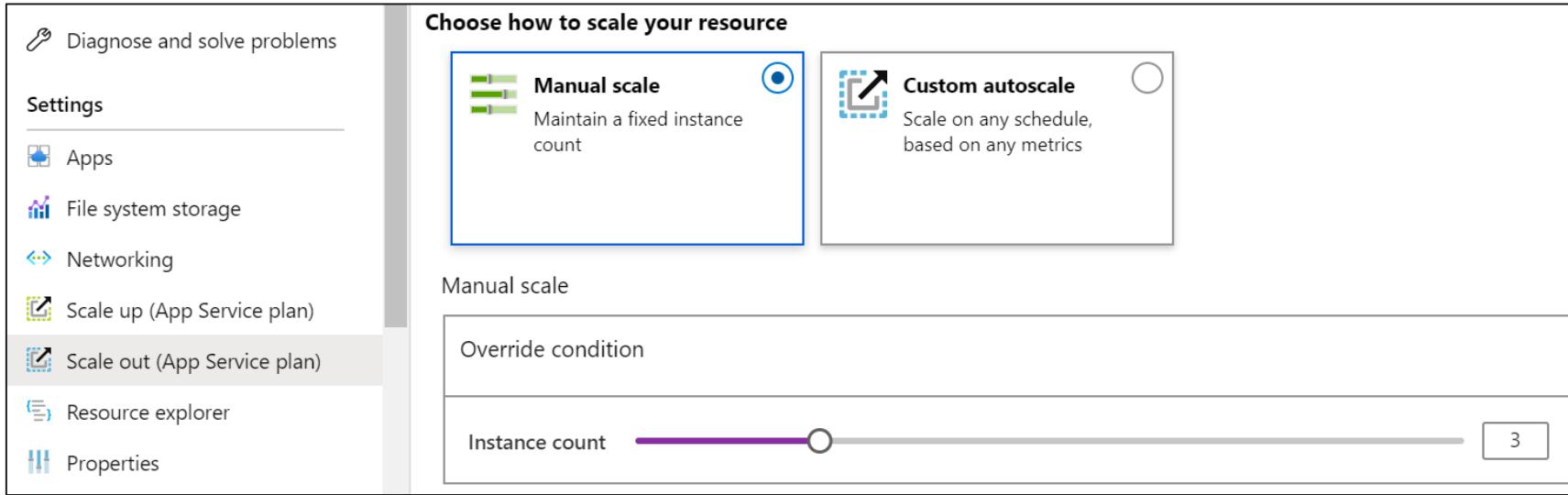
- Define a set of compute resources for a web app to run
- Determines performance, price, and features
- One or more apps can be configured to run in the same App Service plan
- App Service plans define:
 - Region where compute resources will be created
 - Number of virtual machine instances
 - Size of virtual machine instances (Small, Medium, Large)
 - Pricing tier (next slide)

App Service Plan Pricing Tiers

Selected Features	Free	Shared (dev/test)	Basic (dedicated dev/test)	Standard (production workloads)	Premium (enhanced scale and performance)	Isolated (high-performance, security and isolation)
Web, mobile, or API apps	10	100	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB
Auto Scale	–	–	–	Supported	Supported	Supported
Deployment Slots	0	0	0	5	20	20
Max Instances	-	-	Up to 3	Up to 10	Up to 30	Up to 100

- Shared compute (Free and Shared). Run apps on the same Azure VM as other App Service apps, and the resources cannot scale out
- Dedicated compute (Basic, Standard, Premium). Run apps in the same plan in dedicated Azure VMs
- Isolated. Runs apps on dedicated Azure VMs in dedicated Azure virtual networks

App Service Plan Scaling



- Scale up (change the App Service plan)
 - More hardware (CPU, memory, disk)
 - More features (dedicated virtual machines, staging slots, autoscaling)
- Scale out (increase the number of VM instances)
 - Manual (fixed number of instances)
 - Autoscale (based on predefined rules and schedules)

App Service Plan Scale Out

The screenshot shows the 'Default' scale condition settings. It includes a 'Delete warning' message about deleting the last rule, a 'Scale mode' section with 'Scale based on a metric' selected, a 'Rules' section with a note to add a rule (e.g., 'Add a rule that increases instance count by 1 when CPU percentage is above 70%'), and an 'Instance limits' section with minimum, maximum, and default values set to 1, 2, and 1 respectively. A schedule note states: 'This scale condition is executed when none of the other scale condition(s) match'.

- Adjust available resources based on the current demand
- Improves availability and fault tolerance
- Scale based on a metric (CPU percentage, memory percentage, HTTP requests)
- Scale according to a schedule (weekdays, weekends, times, holidays)
- Can implement multiple rules – combine metrics and schedules
- Don't forget to scale down

Azure App Services



Managing App Services Overview

- Azure App Service
- Creating an App Service
- Continuous Deployment
- Deployment Slots
- Creating Deployment Slots
- Securing an App Service
- Custom Domain Names
- Backup an App Service
- Application Insights
- Demonstration – Create an App Service

Azure App Service



.NET



Node.js



PHP



Java



Python (on Linux)



HTML



Custom Windows container (Preview)

- Includes Web Apps API Apps, Mobile Apps, and Function apps
- Fully managed environment enabling high productivity development
- Platform-as-a-service (PaaS) offering for building and deploying highly available cloud apps for web and mobile
- Platform handles infrastructure so developers focus on core web apps and services
- Developer productivity using .NET, .NET Core, Java, Python and a host of others
- Provides enterprise-grade security and compliance

Creating an App Service

- Name must be unique
- Access using *azurewebsites.net* – can map to a custom domain
- Publish Code (Runtime Stack)
- Publish Docker Container
- Linux or Windows
- Region closest to your users
- App Service Plan

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

Subscription * ⓘ Microsoft Azure Internal Consumption

Resource Group * ⓘ (New) rg1 [Create new](#)

Instance Details

Name * your-app-name.azurewebsites.net

Publish * [Code](#) Docker Container

Runtime stack * .NET Core 3.1 (LTS)

Operating System * [Linux](#) [Windows](#)

Region * East US [Not finding your App Service Plan? Try a different region.](#)

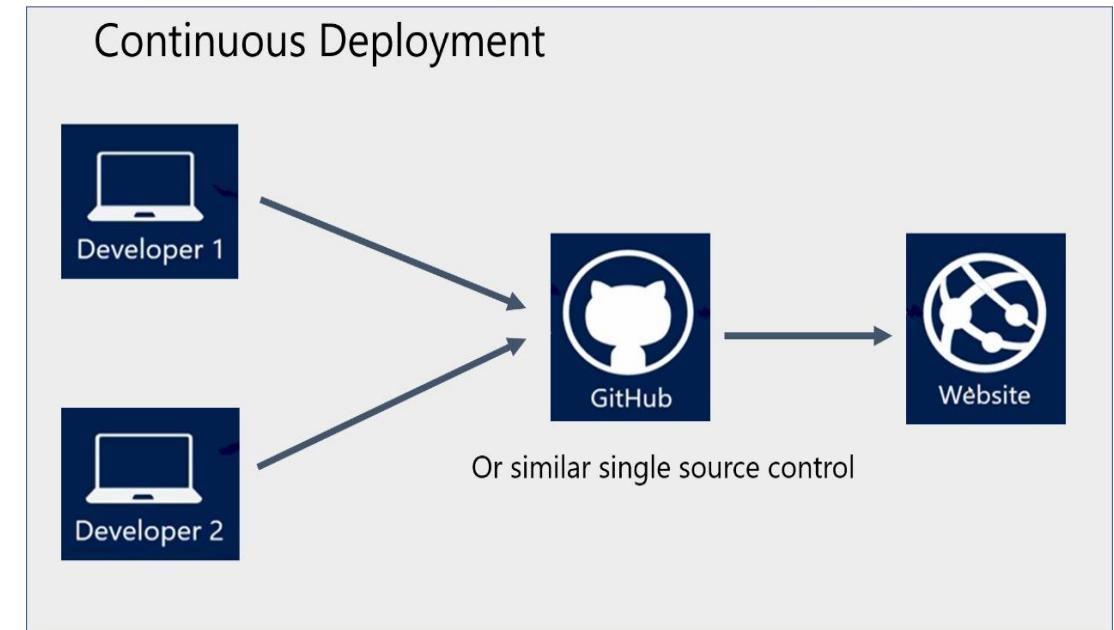
App Service Plan
App Service plan pricing tier determines the location, features, cost and compute resources associated with your app.
[Learn more](#)

Windows Plan (East US) * ⓘ (New) asp1 [Create new](#)

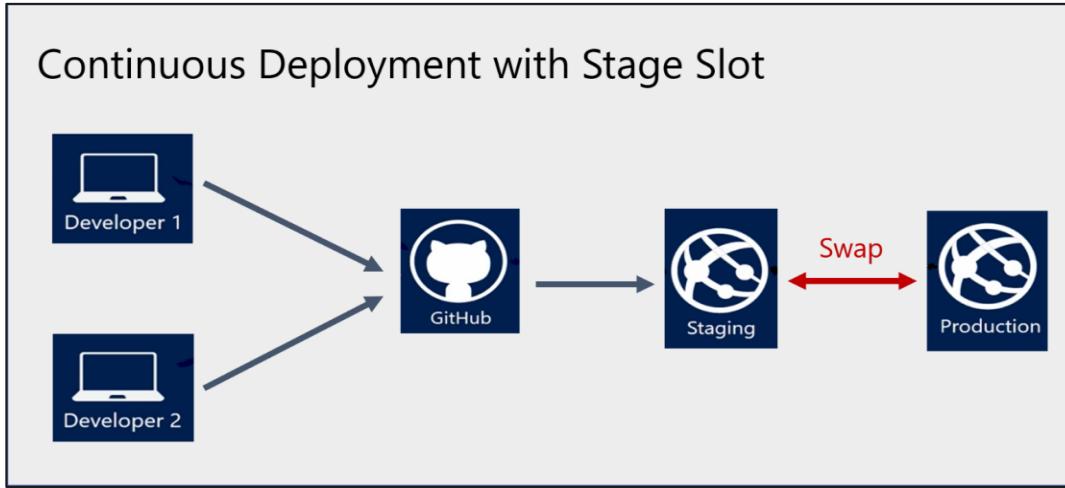
Sku and size * **Standard S1**
100 total ACU, 1.75 GB memory
[Change size](#)

Continuous Deployment

- Work in a single source control
- Whenever code updates are pushed to the source control, then the website or web app will automatically pick up the updates
- A continuous deployment workflow publishes the most recent updates from a project
- Use the portal for continuous deployments from GitHub, Bitbucket, or Azure DevOps



Deployment Slots



Service Plan	Slots
Free, Shared, Basic	0
Standard	Up to 5
Premium	Up to 20
Isolated	Up to 20

- Deploy to a different deployment slots (depends on service plan)
- Validate changes before sending to production
- Deployment slots are live apps with their own hostnames
- Avoids a cold start – eliminates downtime
- Fallback to a last known good site
- Auto Swap when pre-swap validation is not needed

Creating Deployment Slots

- A new slot can be empty or cloned
- When you clone, pay attention to the settings
 - Slot-specific app settings and connection strings
 - Continuous deployment settings
 - App Service authentication settings
- Not all settings are sticky (endpoints, custom domain names, SSL certificates, scaling)
- Review and edit your settings before swapping



Securing an App Service

- Authentication
 - Enable authentication – default anonymous
 - Log in with a third-party identity provider
- Security
 - Troubleshoot with Diagnostic Logs – failed requests, app logging
 - Add an SSL certificate – HTTPS
 - Define a priority ordered allow/deny list to control network access to the app
 - Store secrets in the Azure Key Vault

App Service Authentication

Action to take when request is not authenticated

^

 Protocol Settings

Protocol settings are global and apply to all bindings defined by your app.

HTTPS Only:

Minimum TLS Version:

 TLS/SSL bindings

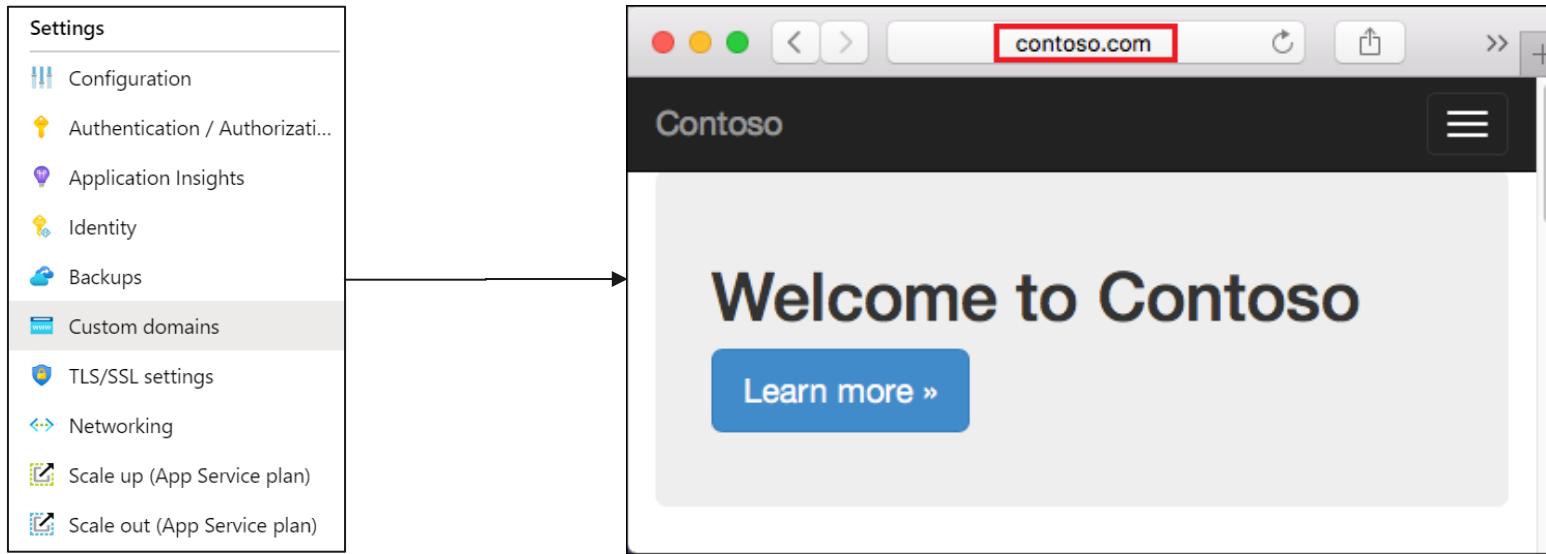
Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valid private certificate (.pfx) issued for the specific hostname. [Learn more](#)

+ Add TLS/SSL Binding

Host name

No TLS/SSL bindings configured for the app.

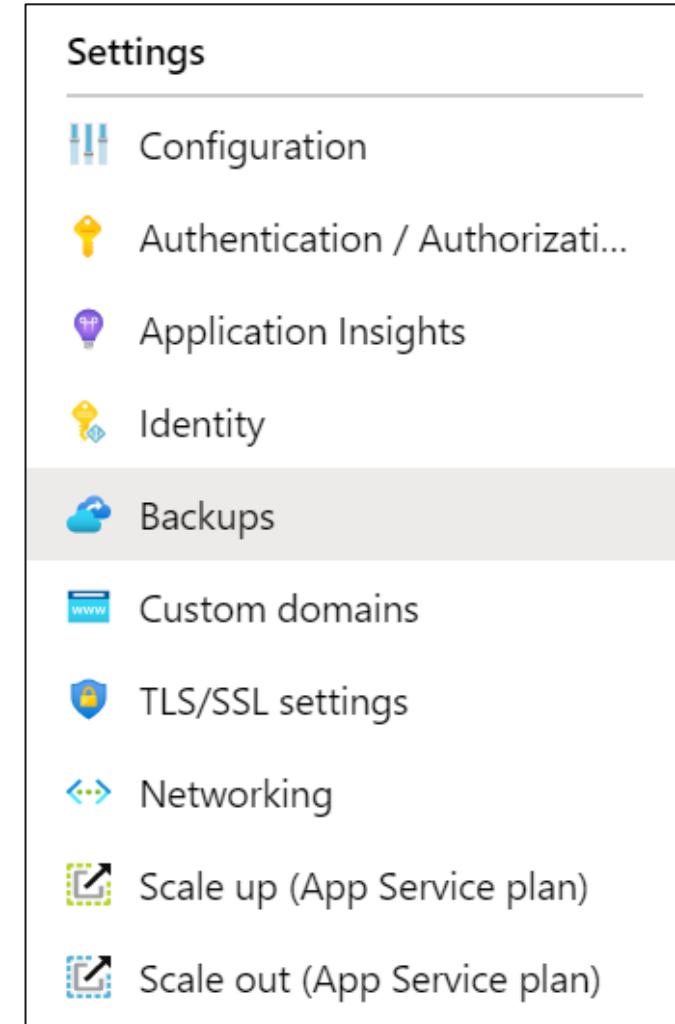
Custom Domain Names



- Redirect the default web app URL
- Validate the custom domain in Azure
- Use the DNS registry for your domain provider – create a CNAME or A record with the mapping
- Ensure App Service plan supports custom domains

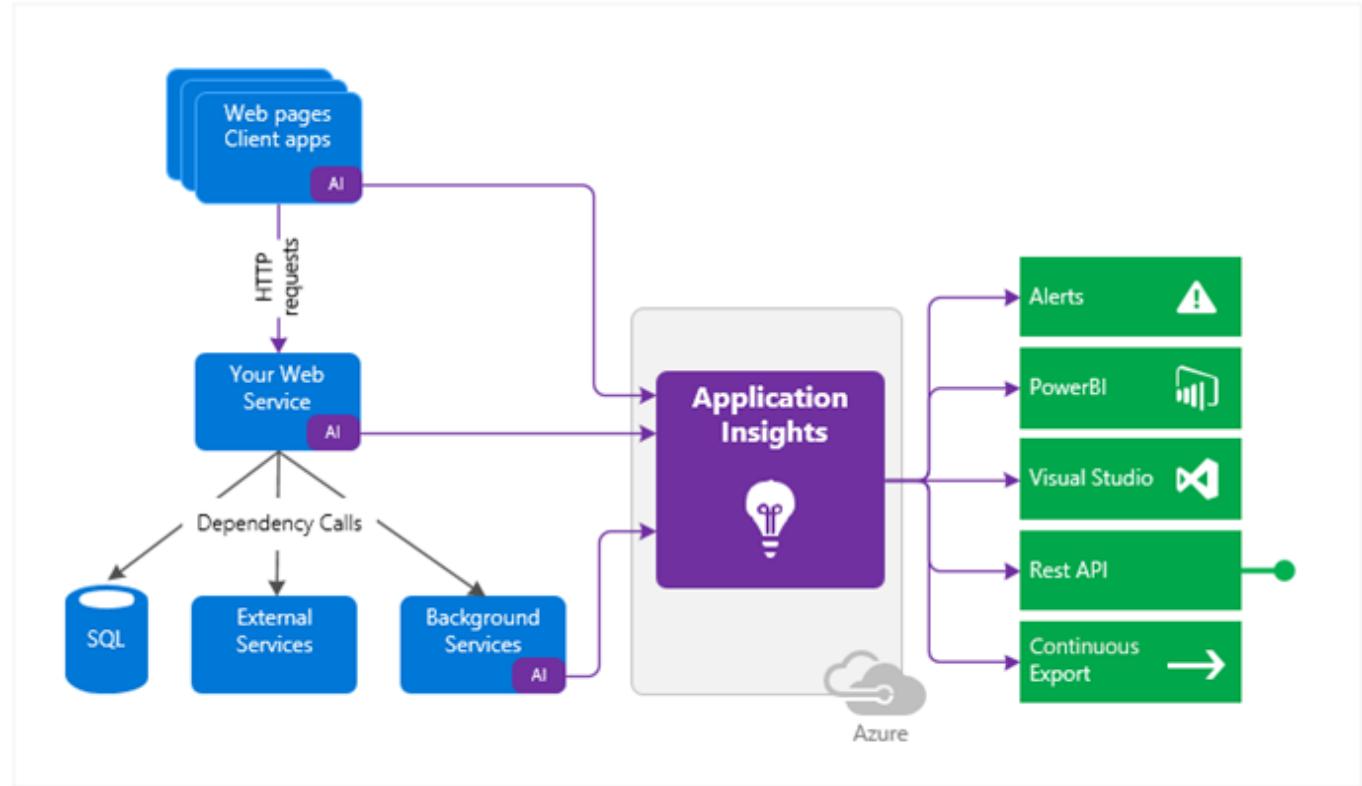
Backup an App Service

- Create app backups manually or on a schedule
- Backup the configuration, file content, and database connected to the app
- Requires Standard or Premium plan
- Backups can be up to 10 GB of app and database content
- Configure partial backups and exclude items from the backup
- Restore your app on-demand to a previous state, or create a new app



Application Insights

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Page views and load performance
- User and session counts
- Performance counters
- Diagnostics and Exceptions



Container Services



Container Services Overview

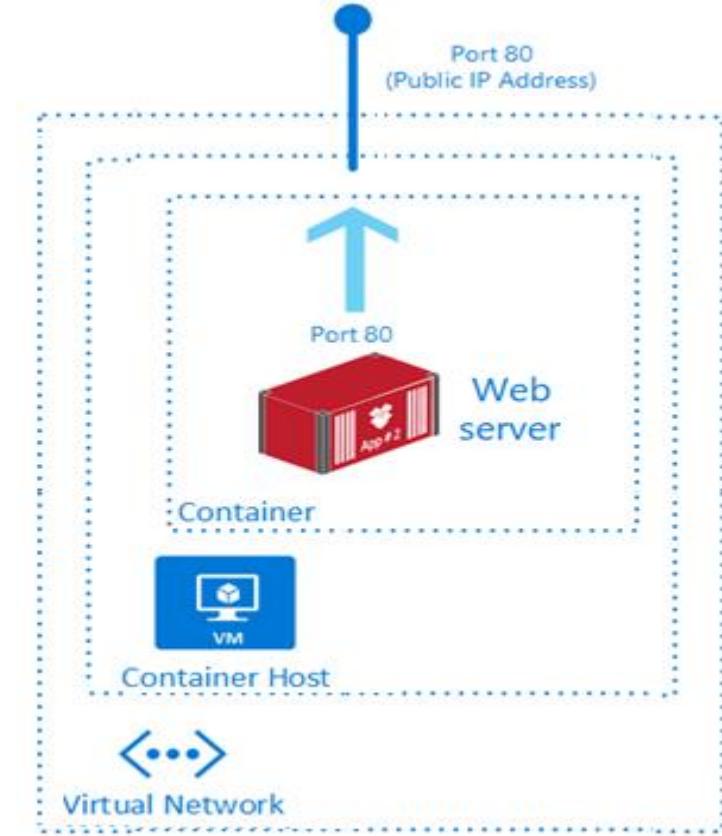
- Containers vs. Virtual Machines
- Azure Container Instances
- Container Groups
- Docker

Containers vs Virtual Machines

Feature	Containers	Virtual Machines
Isolation	Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.	Provides complete isolation from the host operating system and other VMs. This is useful when a strong security boundary is critical, such as hosting apps from competing companies on the same server or cluster.
Operating system	Runs the user mode portion of an operating system and can be tailored to contain just the needed services for your app, using fewer system resources.	Runs a complete operating system including the kernel, thus requiring more system resources (CPU, memory, and storage).
Deployment	Deploy individual containers by using Docker via command line; deploy multiple containers by using an orchestrator such as Azure Kubernetes Service.	Deploy individual VMs by using Windows Admin Center or Hyper-V Manager; deploy multiple VMs by using PowerShell or System Center Virtual Machine Manager.
Persistent storage	Use Azure Disks for local storage for a single node, or Azure Files (SMB shares) for storage shared by multiple nodes or servers.	Use a virtual hard disk (VHD) for local storage for a single VM, or an SMB file share for storage shared by multiple servers.
Fault tolerance	If a cluster node fails, any containers running on it are rapidly recreated by the orchestrator on another cluster node.	VMs can fail over to another server in a cluster, with the VM's operating system restarting on the new server.

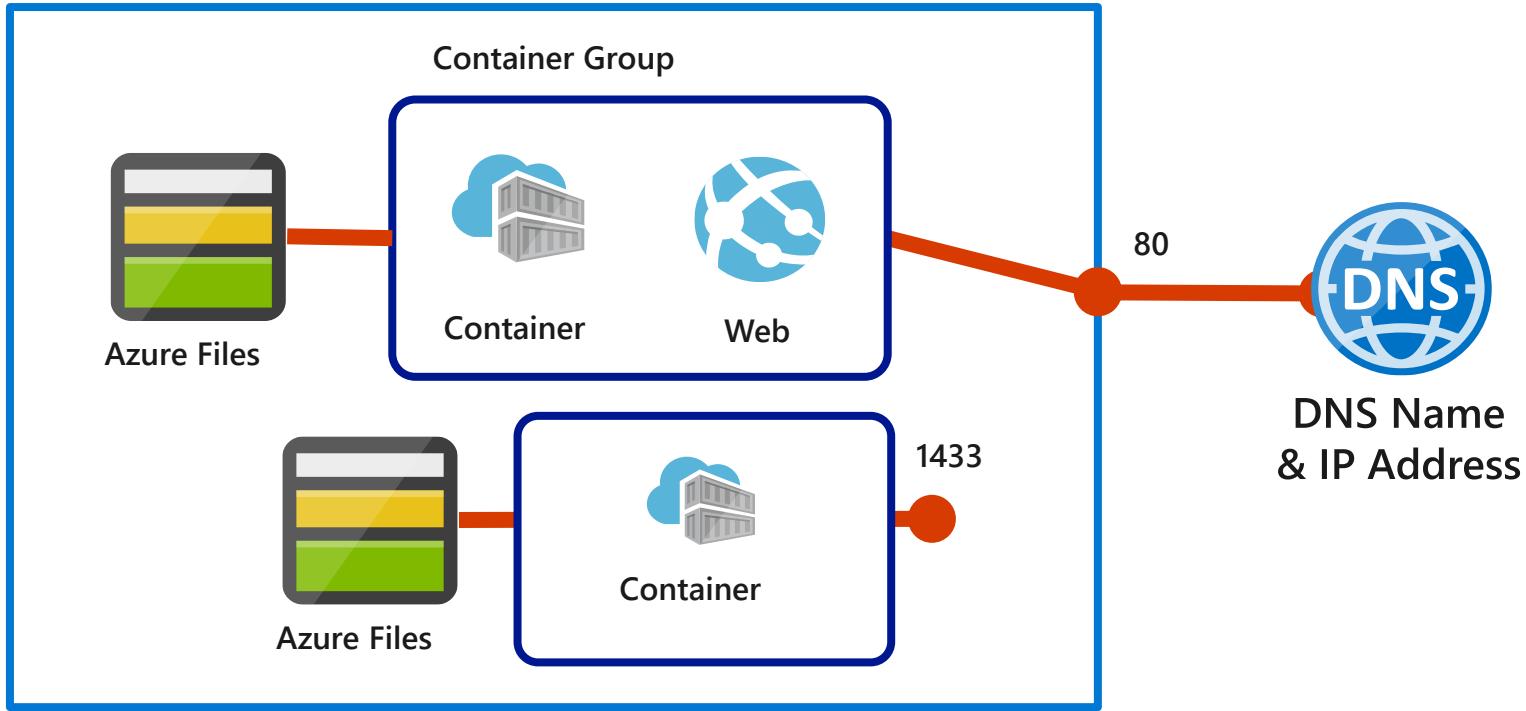
Azure Container Instances

- PaaS Service
- Fast startup times
- Public IP connectivity and DNS name
- Hypervisor-level security
- Isolation features
- Custom sizes
- Persistent storage
- Linux and Windows Containers
- Co-scheduled Groups
- Virtual network Deployment



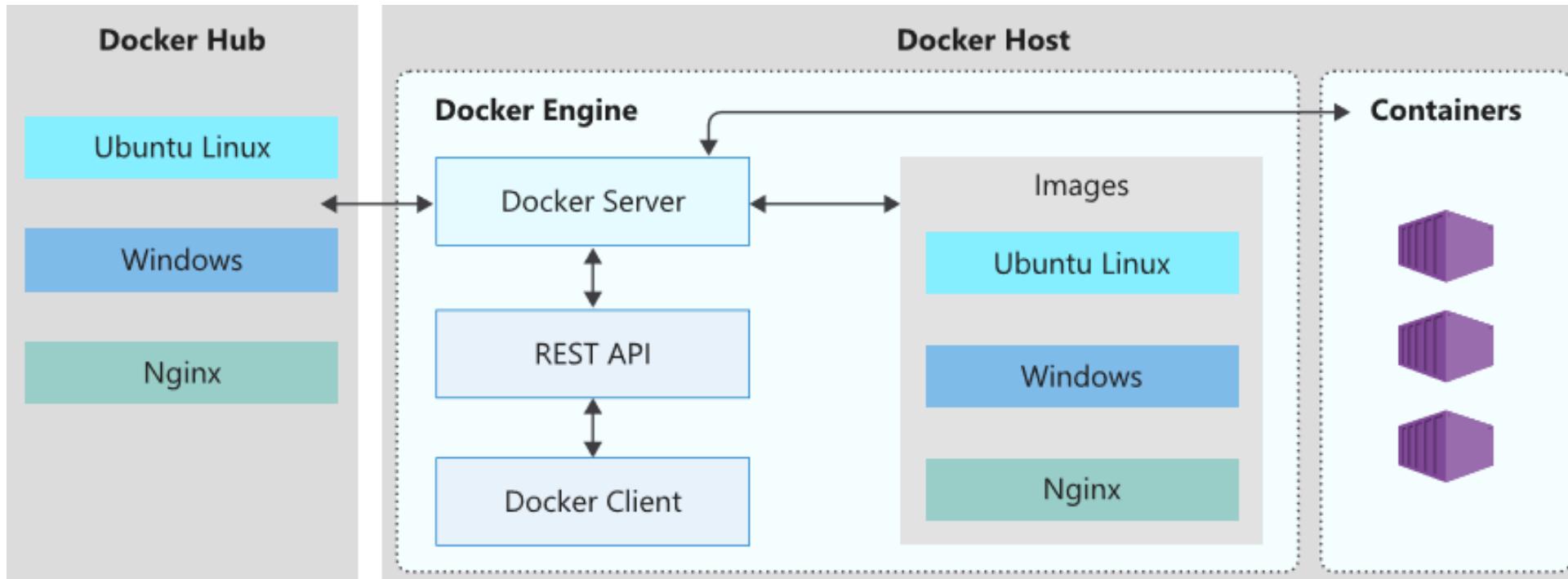
Fastest way to run a container in Azure without provisioning a VM

Container Groups



- Top-level resource in Azure Container Instances
- A collection of containers that get scheduled on the same host
- The containers in the group share a lifecycle, resources, local network, and storage volumes

Docker



- Enables developers to host applications within a container
- A container is a standardized "unit of software" that contains everything required for an application to run
- Available on both Linux and Windows and can be hosted on Azure



AZ-104T00A

Module 10:

Data Protection



Module Overview

- File and Folder Backups
- Virtual Machine Backups

File and Folder Backups



File and Folder Backups Overview

- Azure Backup
- Recovery Service Vault Backup Options
- Implementing On-Premises File and Folder Backups
- Microsoft Azure Recovery Services Agent

Azure Backup

- Azure-based service used to back up and restore data in Microsoft cloud
- Automatic Storage Management
- Multiple storage options
- Unlimited data transfer
- Data encryption
- Application consistent backup
- Long-term retention

Recovery Services Vault Backup Options

- Azure Workloads
- On-Premises workloads

Where is your workload running?

Azure

What do you want to backup?

Virtual machine

- Virtual machine
- Azure FileShare
- SQL Server in Azure VM
- SAP HANA in Azure VM

vmbackuptest- Backup

Recovery Services vault

Where is your workload running?

On-Premises

What do you want to backup?

Files and folders

- Files and folders
- Hyper-V Virtual Machines
- VMware Virtual Machines
- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Exchange
- System State
- Bare Metal Recovery

Step: Prepare Infrastructure

Prepare Infrastructure

Virtual Machine Backups



Virtual Machine Backups Overview

- Virtual Machine Data Protection
- Workload Protection Needs
- Virtual Machine Snapshots
- Recovery Services Vault VM Backup Options
- Implementing VM Backups
- Implementing VM Restore
- Azure Backup Server
- Backup Component Comparison
- Soft Delete
- Azure Site Recovery
- Azure to Azure Architecture

Virtual Machine Data Protection

Snapshots

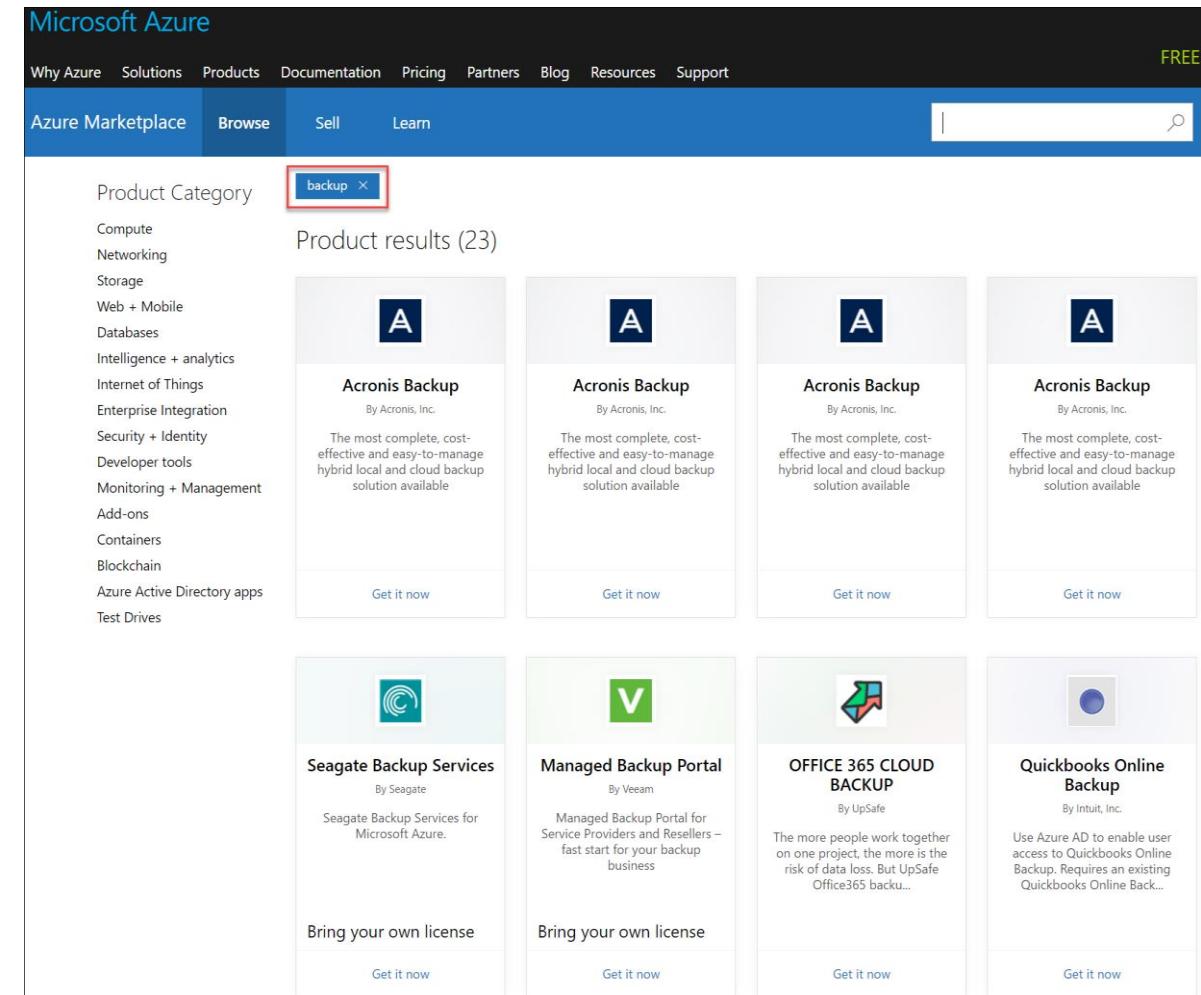
Azure Backup

Azure Site Recovery

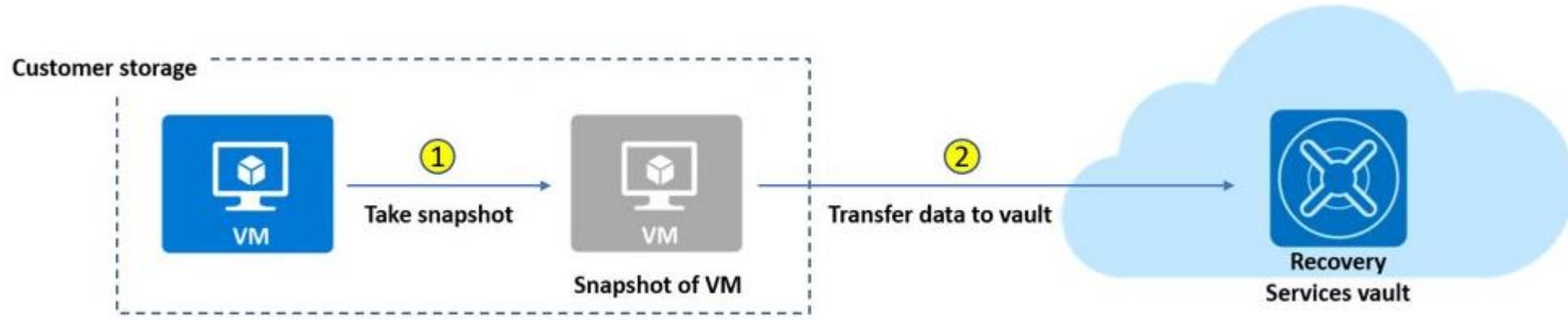
- Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks
- Azure Backup supports application-consistent backups for both Windows and Linux VMs
- Azure Site Recovery protects your VMs from a major disaster scenario when a whole region experiences an outage

Workload Protection Needs

- Many backup options are available
- How the workload is being protected today?
- How often is the workload is backed up?
- What types of backups are being done?
- Is disaster recovery protection in place?



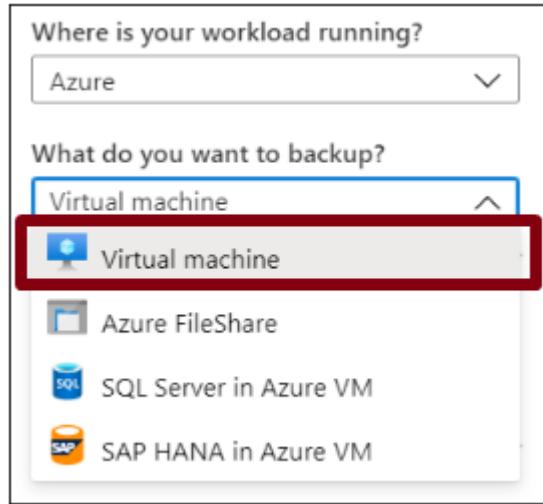
Virtual Machine Snapshots



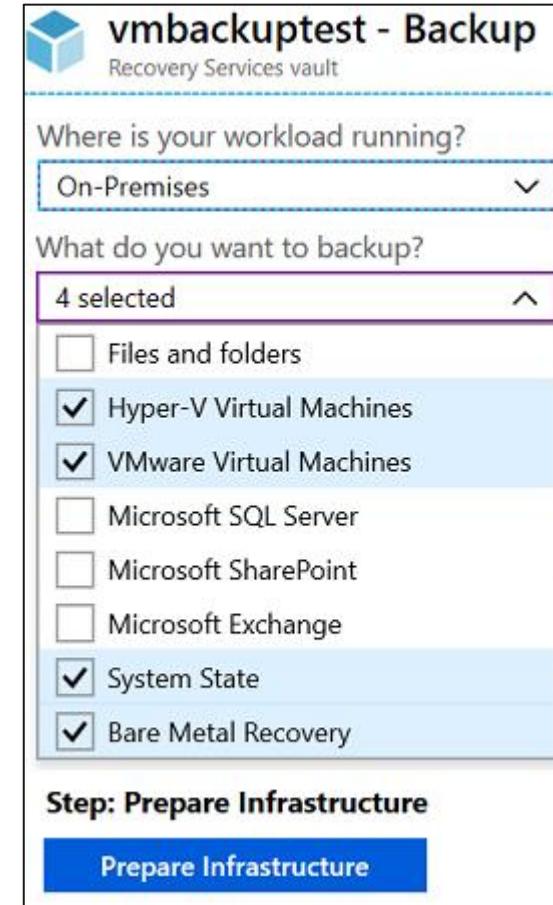
- Use snapshots taken as part of a backup job
- Reduces recovery wait times – don't wait for data transfer to the vault to finish
- Configure Instant Restore retention (1 to 5 days)

Recovery Services Vault VM Backup Options

Azure Workloads

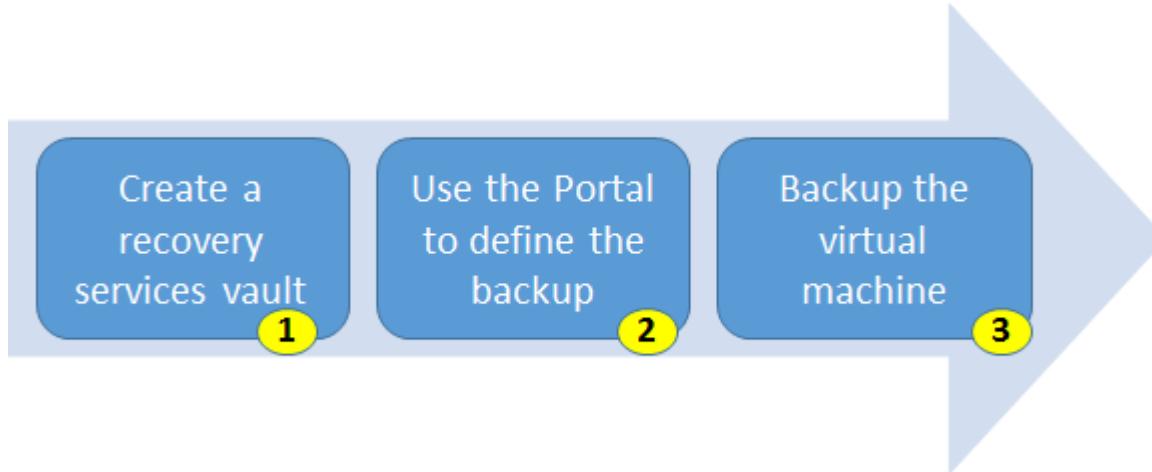


On-Premises Workloads



- ✓ Multiple servers can be protected using the same Recovery Services vault

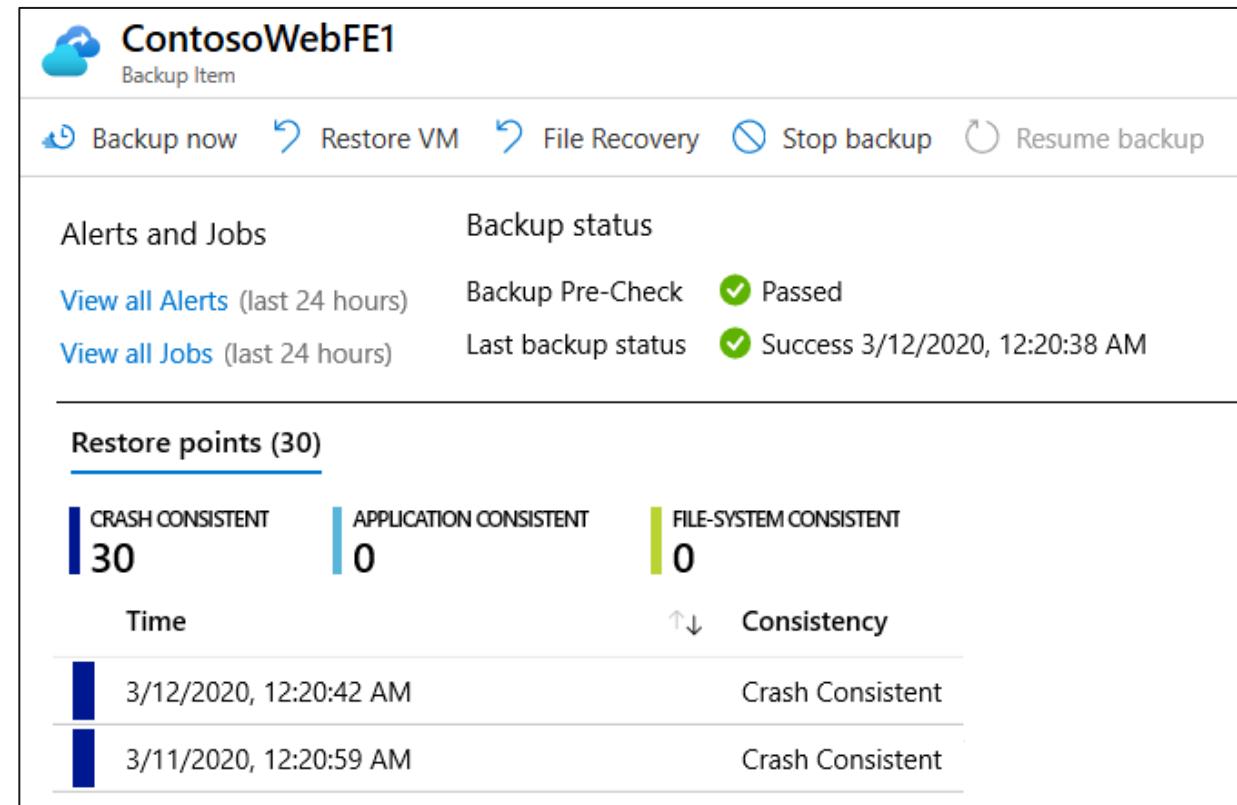
Implementing VM Backups



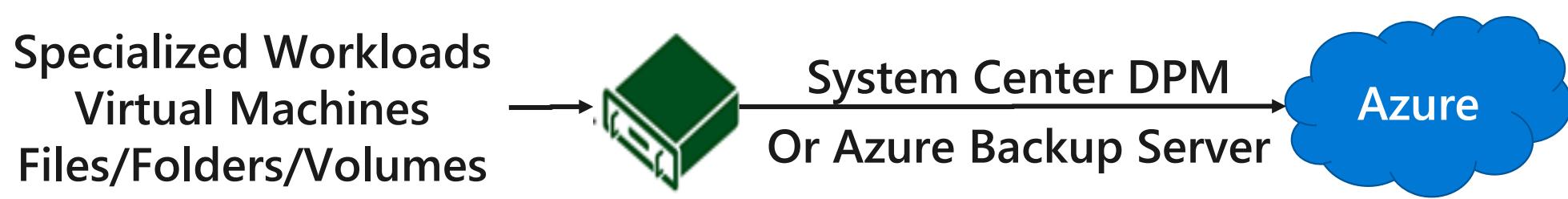
1. Use a Recovery Services Vault in the region where you are performing your Virtual Machine backups and choose a replication strategy for the Vault.
2. Take snapshots (recovery points) of your data at defined intervals. These snapshots are stored in recovery services vaults.
3. For the Backup extension to work, the Azure VM Agent must be installed on the Azure virtual machine.

Implementing VM Restore

- Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation
- The Backup service also creates and temporarily displays notifications, so you monitor how the backup is proceeding



Azure Backup Server



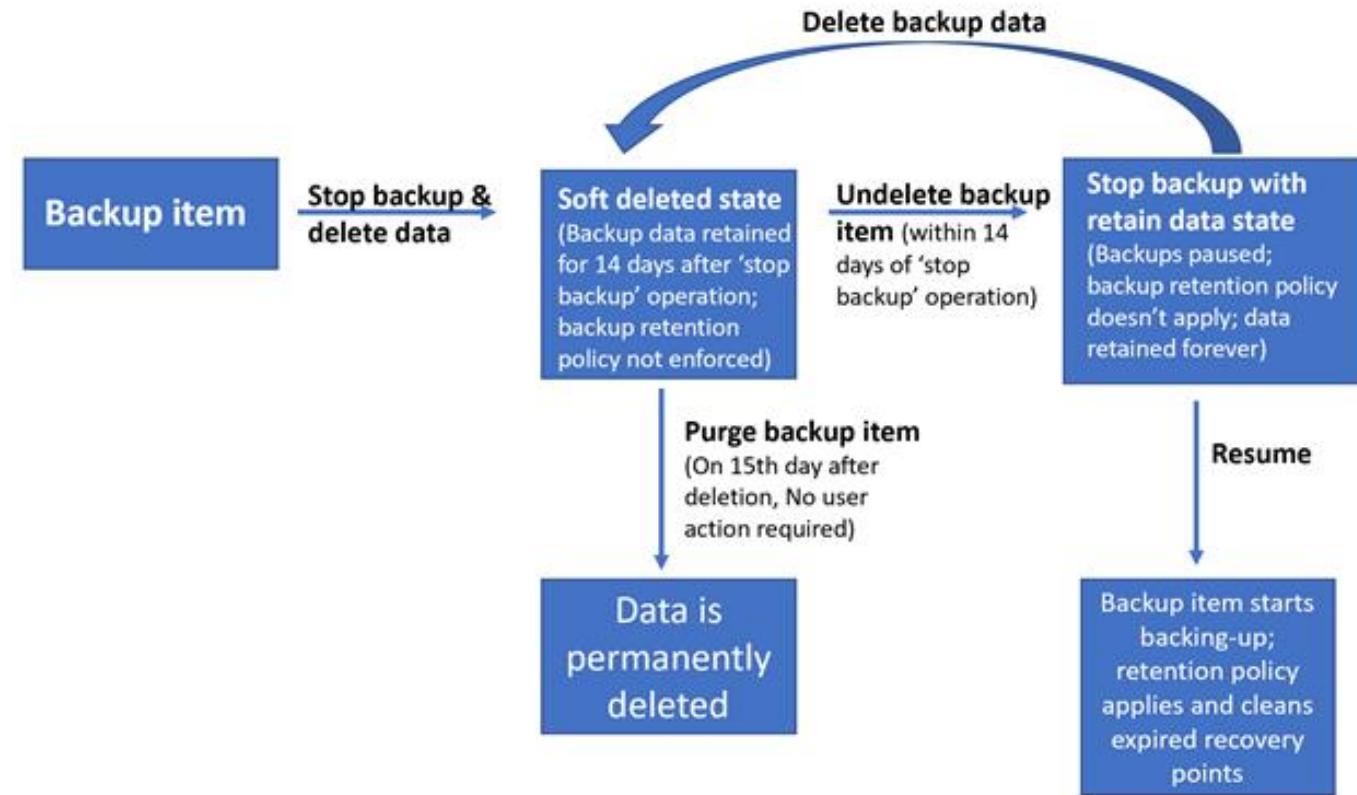
- App-aware backups, file/folder/volume backups, and machine state backups (bare-metal, system state)
- Each machine runs the DPM/MABS protection agent, and the MARS agent runs on the MABS/DPM
- Flexibility and granular scheduling options
- Manage backups for multiple machines in a protection group

Backup Component Comparison

Component	Benefits	Limits	Protects	Backup Storage
Azure Backup (MARS) agent	<ul style="list-style-type: none">Backup files and folders on physical or virtual Windows OSNo separate backup server required.	<ul style="list-style-type: none">Backup 3x per dayNot application awareFile, folder, and volume-level restore onlyNo support for Linux	<ul style="list-style-type: none">FilesFolders	<ul style="list-style-type: none">Recovery services vault
Azure Backup Server	<ul style="list-style-type: none">App aware snapshotsFull flex for when to backupsRecovery granularityLinux support on Hyper-V and VMware VMsBackup and restore VMware VMsDoesn't require a System Center license	<ul style="list-style-type: none">Cannot backup Oracle workloadsAlways requires live Azure subscriptionNo support for tape backup	<ul style="list-style-type: none">FilesFolders,VolumesVMsApplicationsWorkloads	<ul style="list-style-type: none">Recovery services vaultLocally attached disk

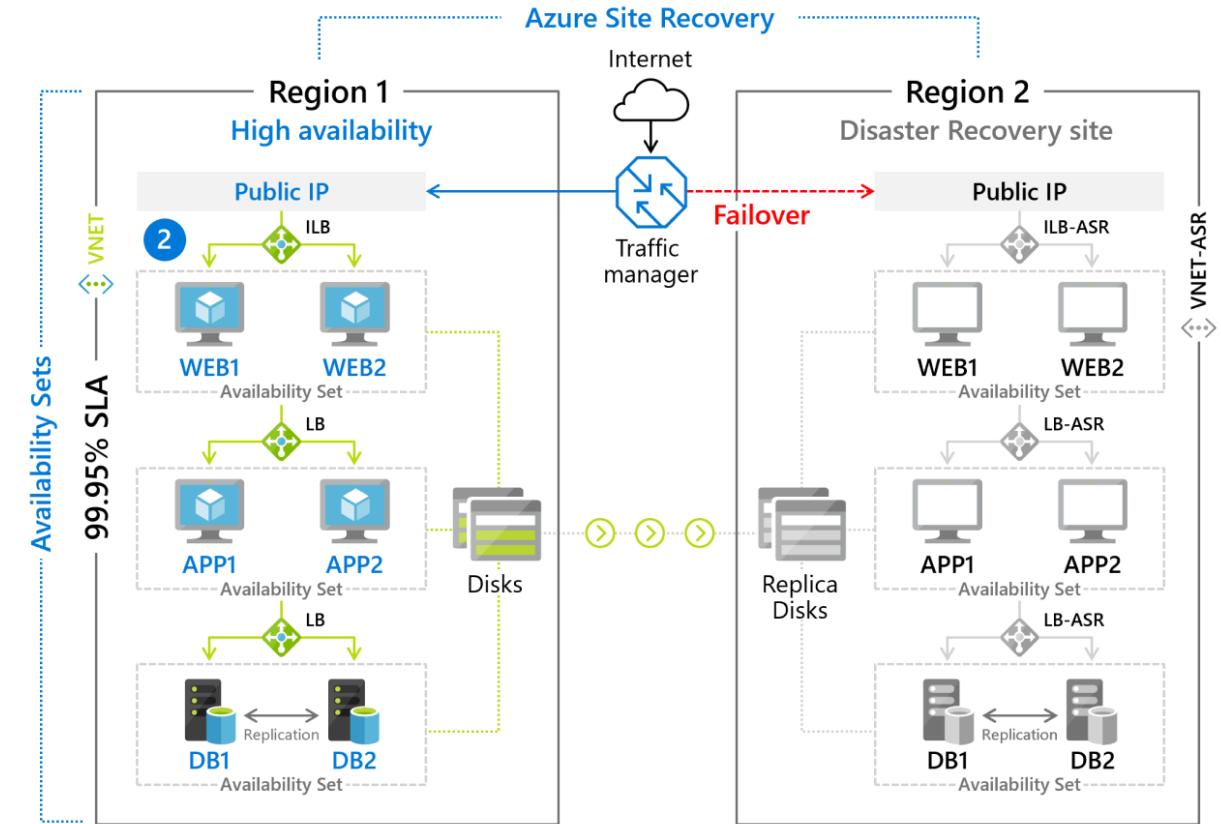
Soft Delete

- Backup data is retained for 14 additional days
- Recover soft deleted backup items using an 'Undelete' operation
- Natively built-in for all the recovery services vaults

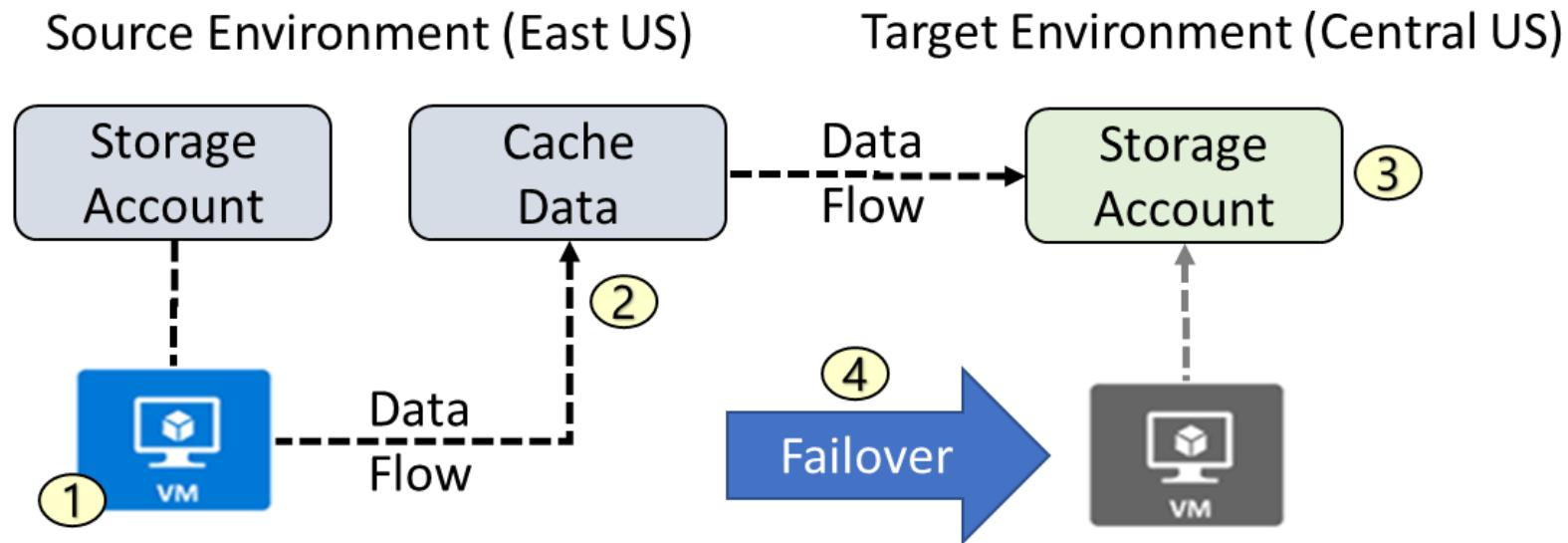


Azure Site Recovery

- Replicate Azure VMs from one Azure region to another
- Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure
- Replicate AWS Windows instances to Azure
- Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site



Azure to Azure Architecture



1. VM is registered with Azure Site Recovery
2. Data is continuously replicated to cache
3. Cache is replicated to the target storage account
4. During failover the virtual machine is added to the target environment

Module 10 Lab and Review



AZ-104T00A

Module 11:

Monitoring



Module Overview

- Azure Monitor
- Azure Alerts
- Log Analytics
- Network Watcher

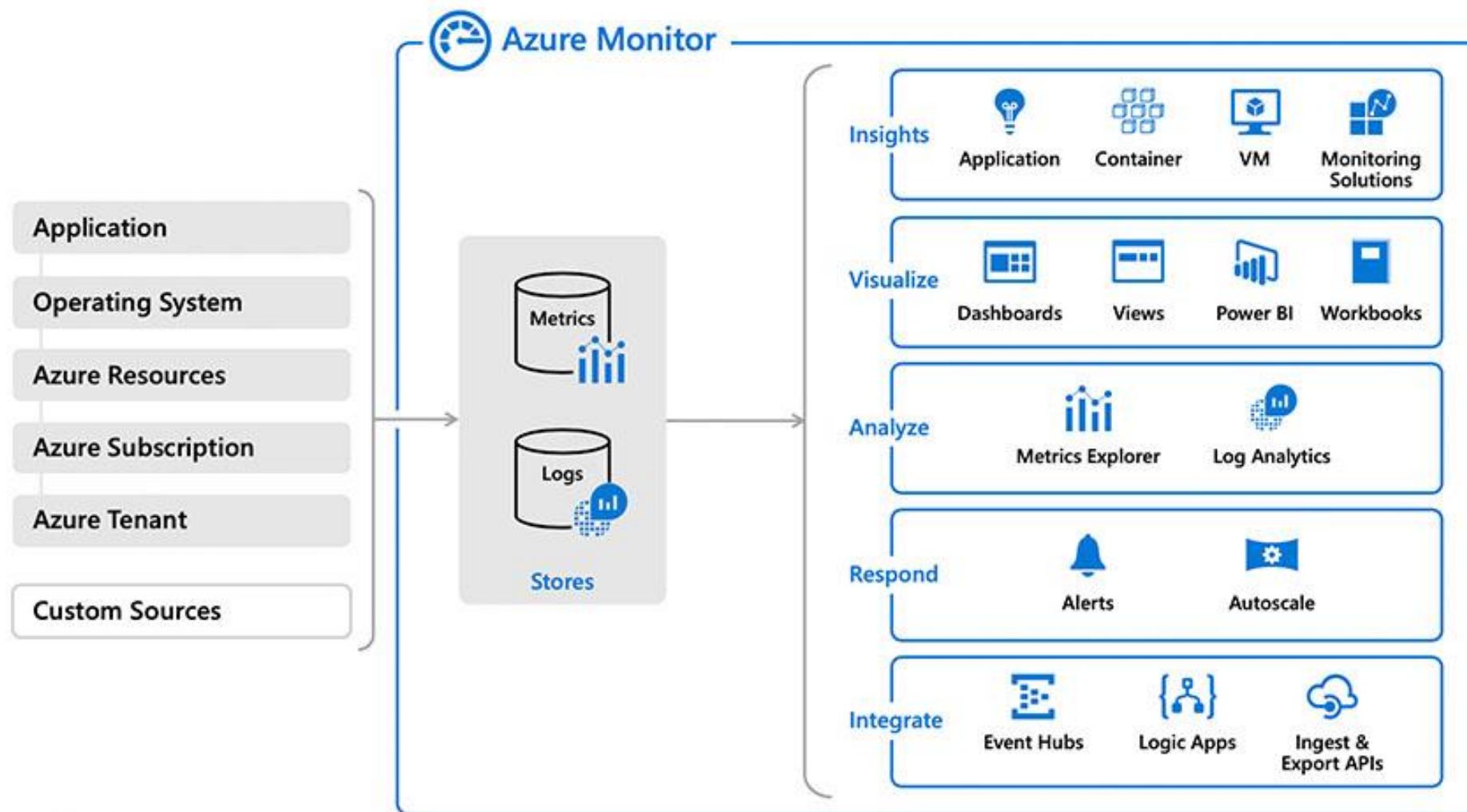
Azure Monitor



Azure Monitor Overview

- Azure Monitor Service
- Key Capabilities
- Monitoring Data Platform
- Log Data
- Data Types
- Azure Advisor
- Activity Log
- Query the Activity Log

Azure Monitor Service

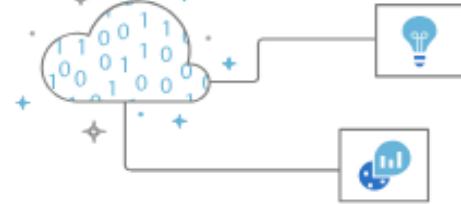


Key Capabilities



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](#)

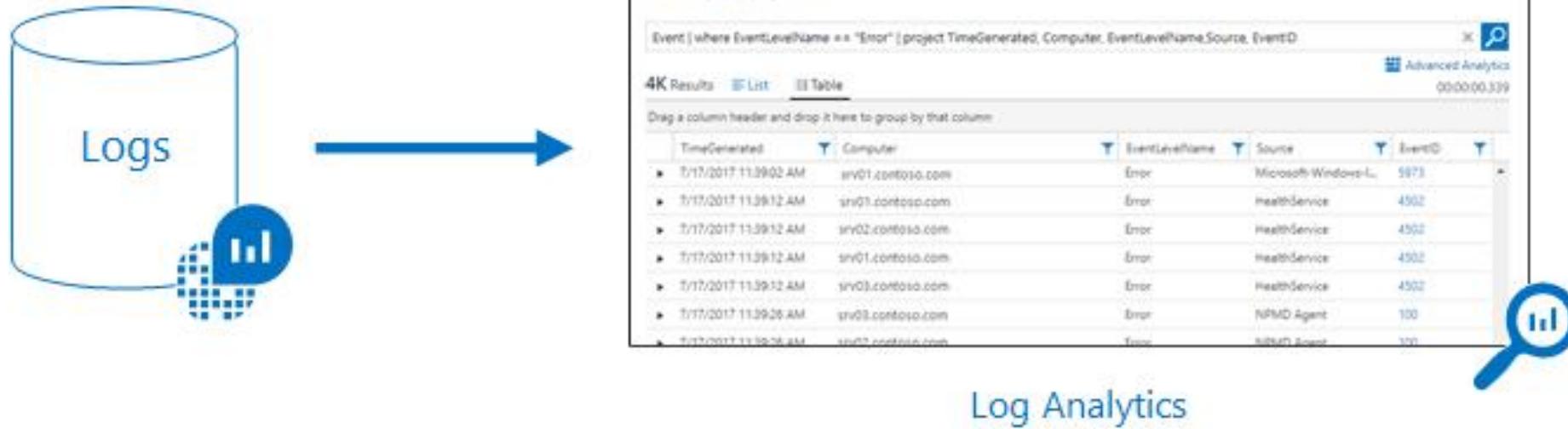
- Core monitoring for Azure services
- Collects metrics, activity logs, and diagnostic logs
- Use for time critical alerts and notifications

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



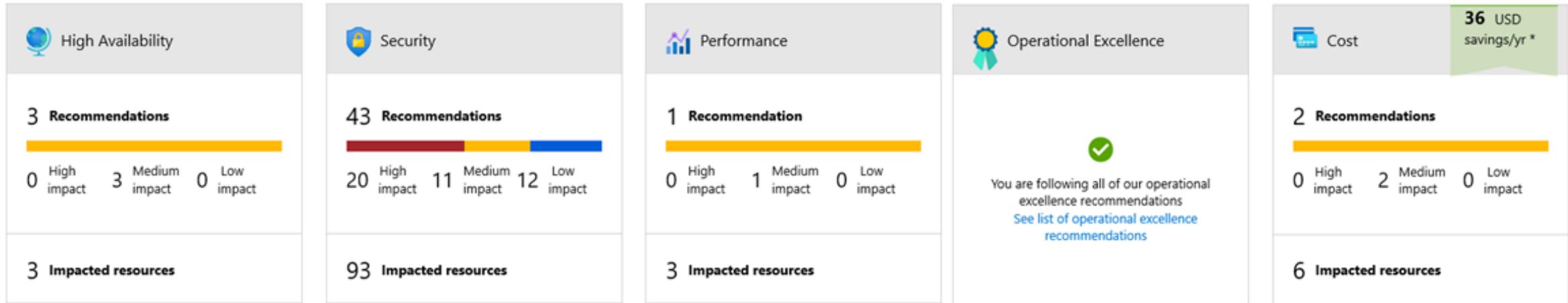
Log Analytics

- 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

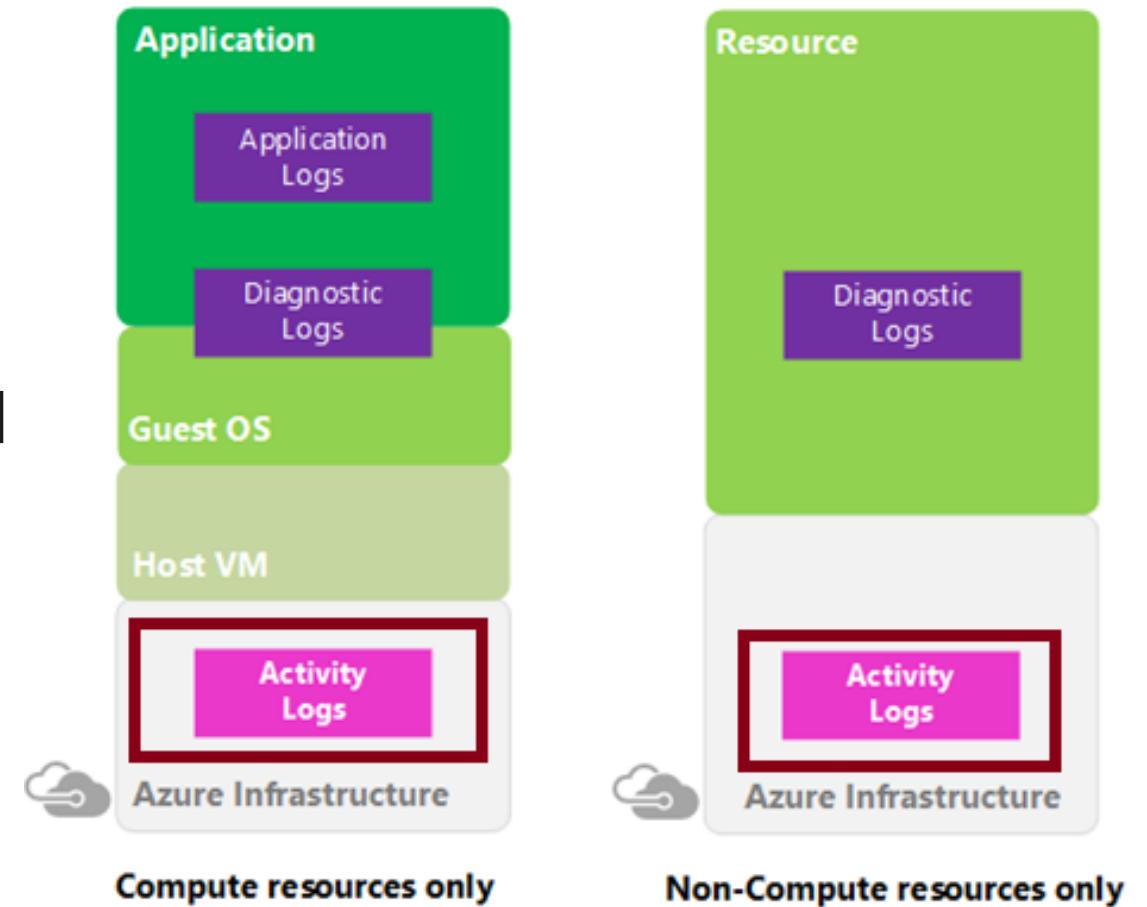
Azure Advisor



- 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

The screenshot shows the 'Activity log' blade in the Azure portal. At the top, there are navigation links: 'Edit columns', 'Refresh', 'Diagnostics settings', 'Download as CSV', 'Logs', and 'Pin current filters'. Below these are search and filter controls: a 'Search' bar, 'Quick Insights', and an 'Add Filter' button. There are also buttons for 'Management Group : None', 'Subscription : 2 selected', 'Timespan : Last 6 hours', and 'Event severity : All'. The main area displays a table of operations:

Operation name	Status	Time	Time stamp	Subscription
> ! Create or Update Virtual Network Subnet	Failed	a minute ago	Thu Mar 12 ...	ASC DEMO
> i Write GuestConfigurationAssignments	Succeeded	17 minutes ...	Thu Mar 12 ...	ASC DEMO
> i Gets workflow recommend operation groups	Succeeded	29 minutes ...	Thu Mar 12 ...	ASC DEMO

- 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

Azure Alerts



Azure Alerts Overview

- Azure Monitor Alerts
- Creating Alert Rules
- Action Groups

Azure Monitor Alerts

Alerts

New alert rule Manage alert rules Manage actions View classic alerts Refresh Provide feedback

Total alerts	Smart groups (Preview)	Total alert rules	Action rules (preview)	
1179 Since 2/11/2020, 11:07:58 AM	3 99.75% Reduction	9 Enabled 7	0 Enabled 0	
Severity	Total Alerts	New	Acknowledged	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0
Sev 2	0	0	0	0
Sev 3	1178	1178	0	0
Sev 4	1	1	0	0

- Unified authoring experience
- Displayed by severity
- Categorized by New, Acknowledged, and Closed

Creating Alert Rules

1. Resource: Target selection, Alert criteria, and Alert logic
2. Condition: Alert rule name, description, and severity (0 to 4)
3. Action group: notify your team via email and text messages or automate actions using webhooks and runbooks

Create rule
Rules management

*** RESOURCE**
Select the target(s) that you wish to monitor
Select

*** CONDITION**
No condition defined, click on 'Add condition' to select a signal and define its logic
Add condition

ACTION GROUPS
Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
No action group selected	

Select existing **Create New**

Action Groups

- Notifies a group of users that an alert has been triggered
- Is a collection of notification preferences

Add action group

Action group name *	Sample action group
Short name *	SampleAG
Subscription *	Visual Studio Enterprise
Resource group *	Default-ActivityLogAlerts (to be created)
Actions	
Action name *	Action Type *
Unique name for the action	Select an action type
<ul style="list-style-type: none">Automation RunbookAzure FunctionEmail Azure Resource Manager RoleEmail/SMS/Push/VoiceITSMLogicAppSecure WebhookWebhook	

Log Analytics



Log Analytics Overview

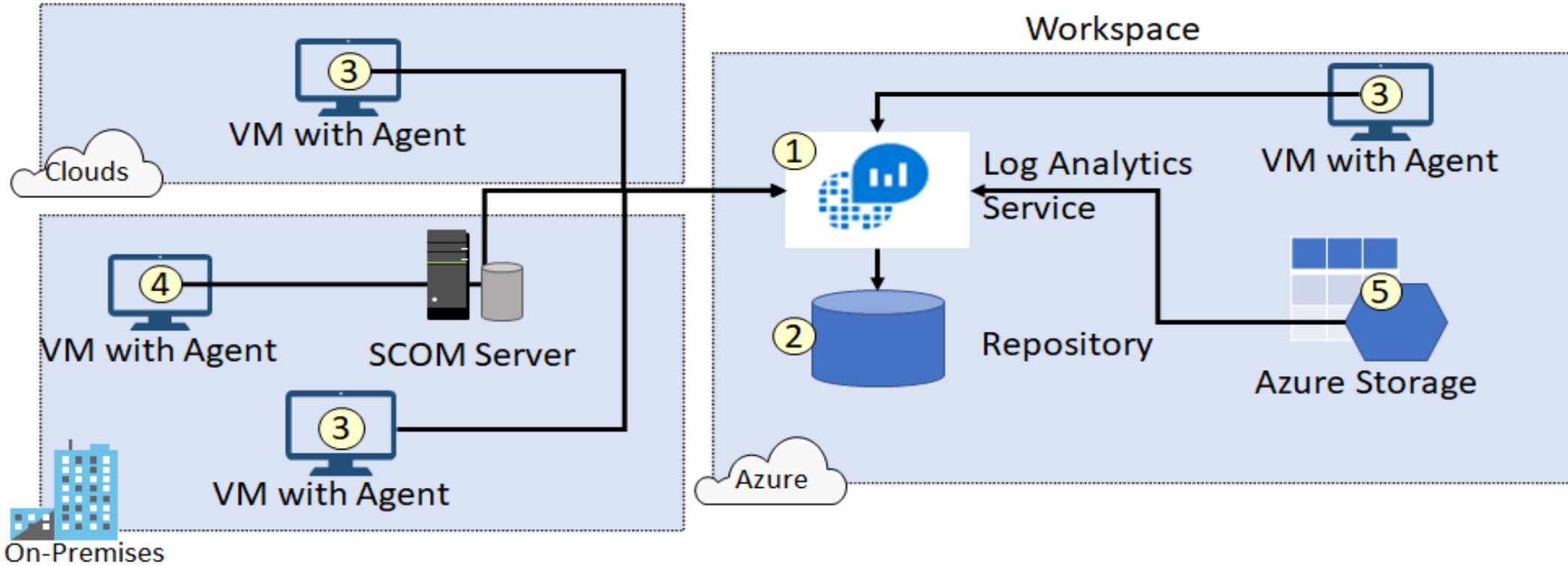
- Log Analytics
- Create a Workspace
- Connected Sources
- Data Sources
- Log Analytics Querying
- Query Language Syntax

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

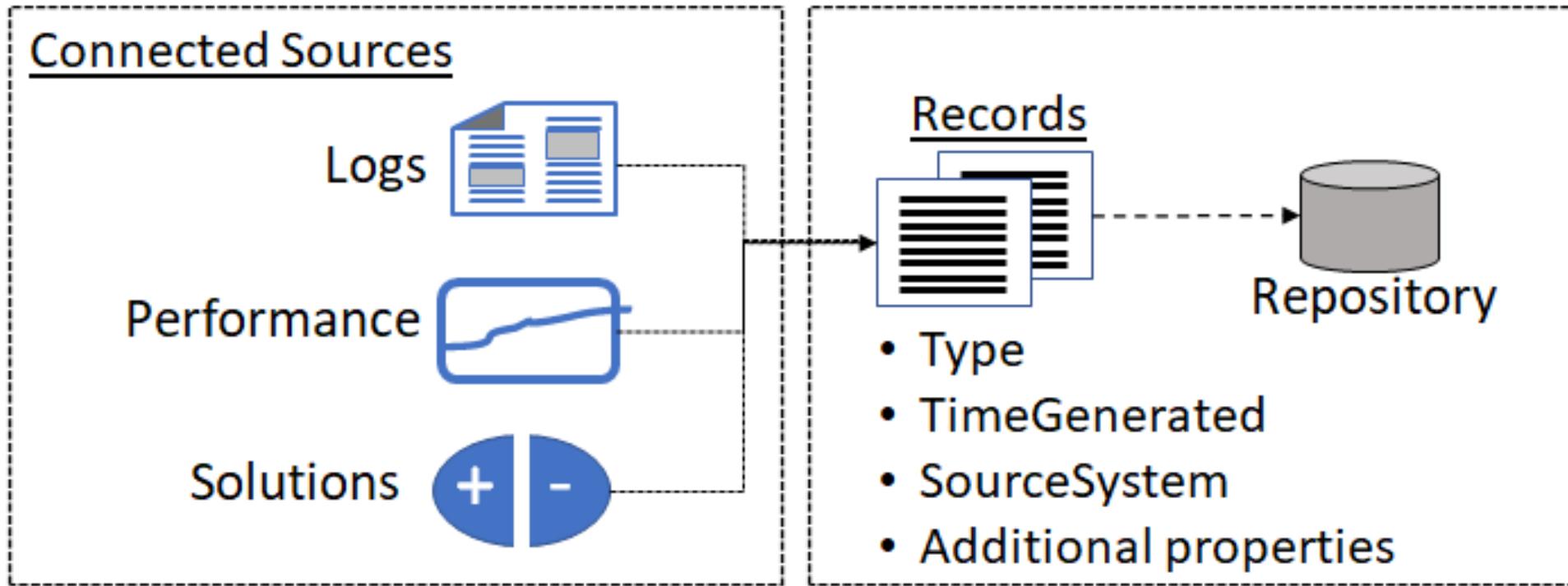
The screenshot shows the Microsoft Monitor - Logs interface. At the top is a search bar labeled "Search (Ctrl+ /)". Below it are several navigation links: "Overview", "Activity log", "Alerts", "Metrics", and "Logs". The "Logs" link is highlighted with a red box. To the right of these links is a sidebar titled "Active" which lists various logs under the "contosoretail-IT" resource group, such as ADAssessment, ADReplication, AlertManagement, AntiMalware, ApplicationInsights, AzureAutomation, ChangeTracking, CompatibilityAssessment, ContainerInsights, Containers, DeviceHealthProd, DnsAnalytics, InfrastructureInsights, and LogManagement.

Connected Sources



- Connected Sources generate data
- Data can be collected from Windows, Linux, SCOM and Azure Storage

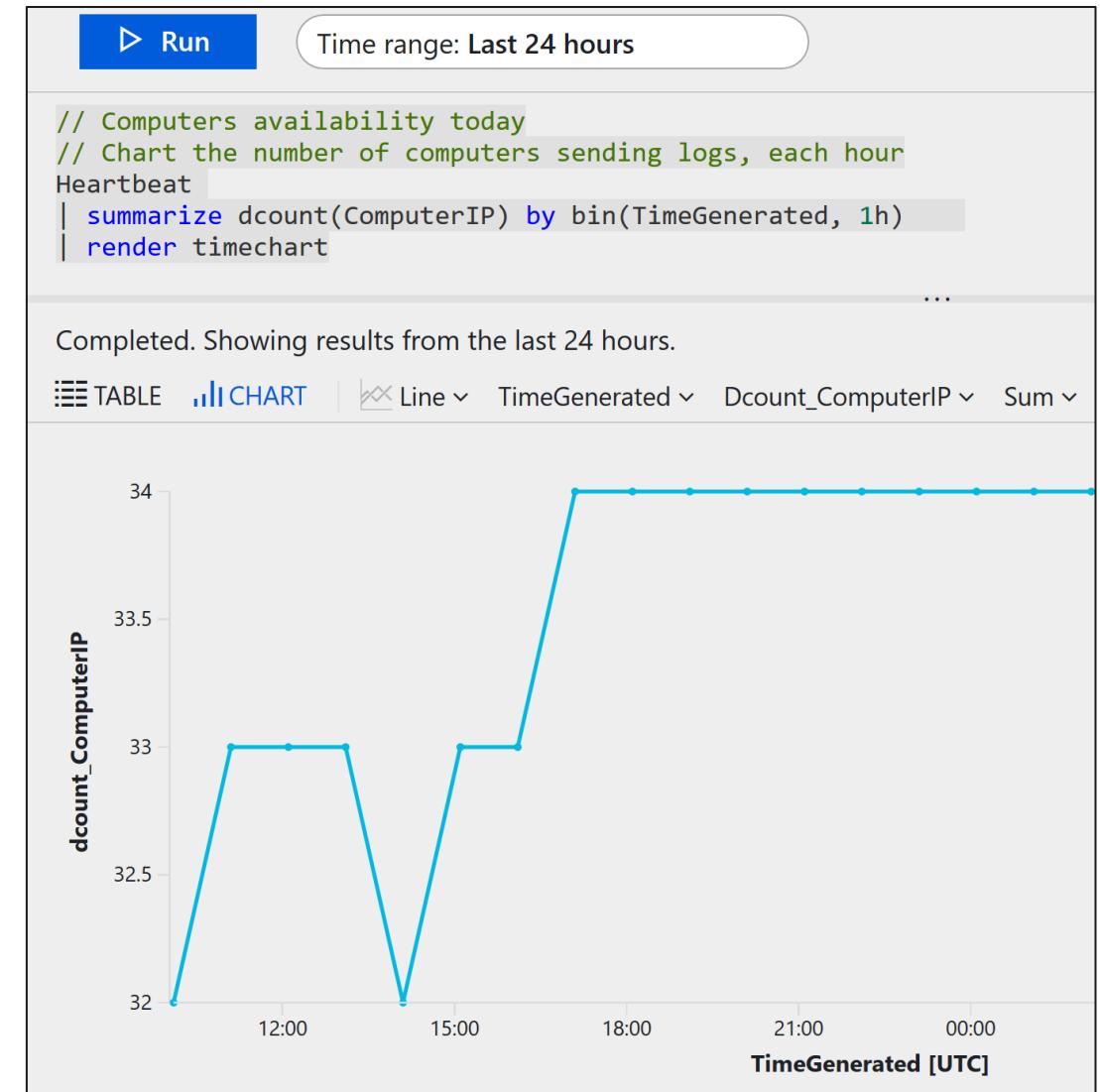
Data Sources



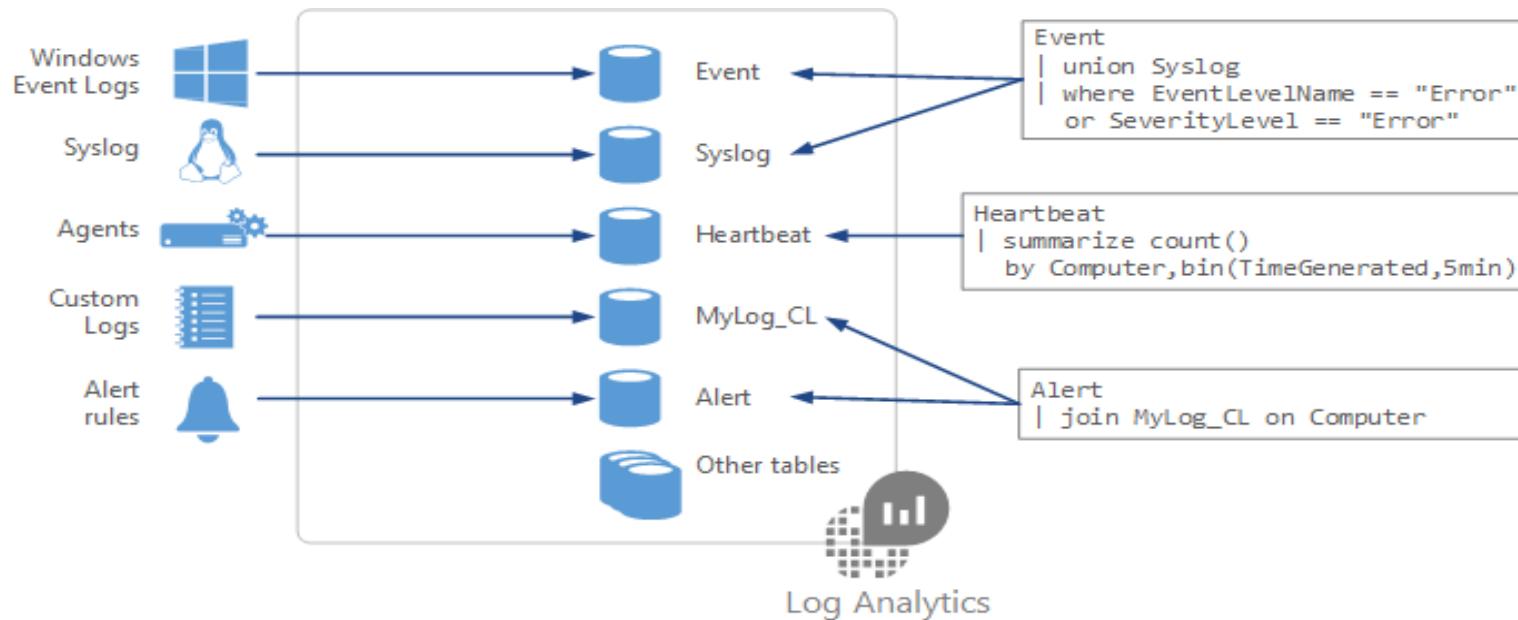
- Data sources include: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog.
- Each data source has additional configuration options.

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
```

Network Watcher

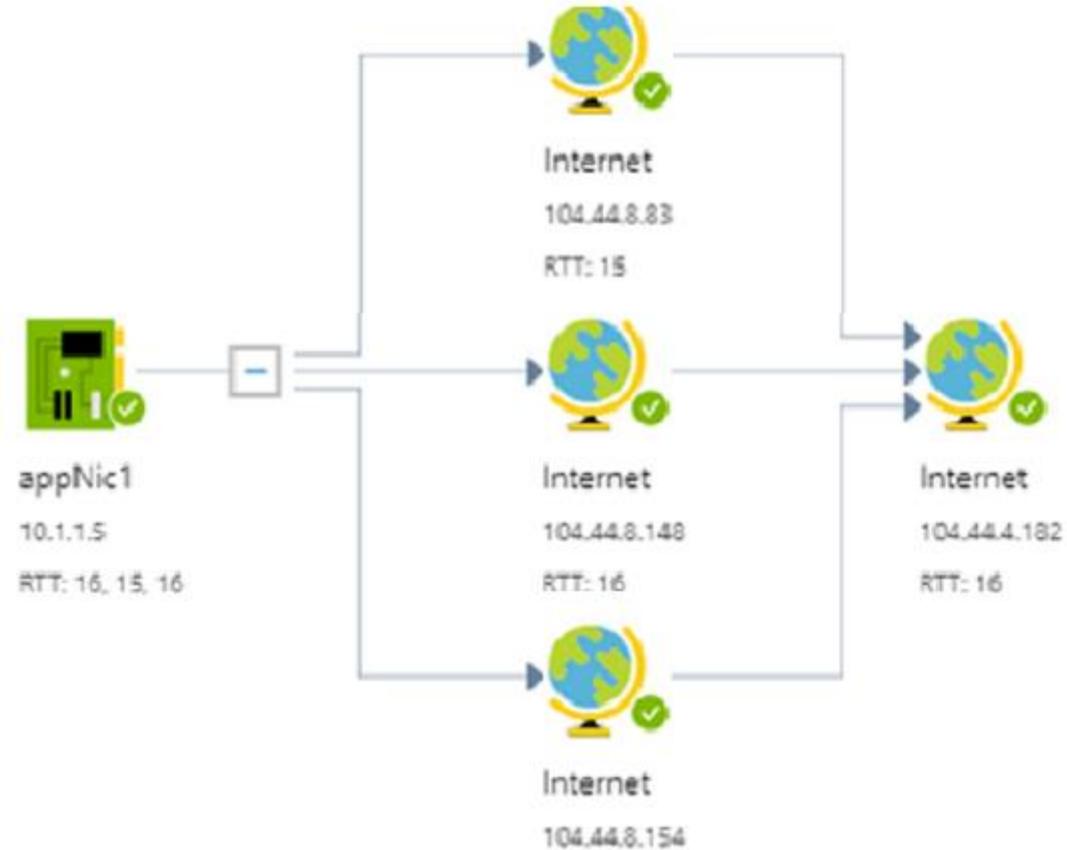


Network Watcher Overview

- 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

Network Watcher	
Monitoring	Network diagnostic tools
 Topology	 IP flow verify
 Connection monitor	 Next hop
 Network Performance Monitor	 Effective security rules
Logs	
 NSG flow logs	 VPN troubleshoot
 Diagnostic logs	 Packet capture
 Traffic Analytics	 Connection troubleshoot

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.

The screenshot shows the Azure IP Flow Verify diagnostic tool interface. On the left, there's a sidebar with 'Network diagnostic tools' (IP flow verify, Next hop, Effective security rules, VPN troubleshoot, Packet capture, Connection troubleshoot) and sections for Metrics (Usage + quotas) and Logs (NSG flow logs, Diagnostic logs, Traffic Analytics). The main area is titled 'Packet details' and contains fields for Protocol (TCP selected), Direction (Inbound selected), Local IP address (10.1.1.4), Local port (3389), Remote IP address (13.24.35.46), and Remote port (3389). A 'Check' button is present. Below it, an error message says 'Access denied' with a red exclamation mark icon. At the bottom, it specifies the security rule as 'DenyAllInBound'.

Packet details	
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Direction	<input checked="" type="radio"/> Inbound <input type="radio"/> Outbound
Local IP address *	10.1.1.4
Local port *	3389
Remote IP address *	13.24.35.46
Remote port *	3389

Check

Access denied

Security rule
DenyAllInBound

Diagnostics - Next Hop

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

Subscription * ⓘ
MSDN Platforms Subscription

Resource group * ⓘ
Demo

Virtual machine * ⓘ
vm01

Network interface * ⓘ
vm01165

Source IP address * ⓘ
10.1.1.4

Destination IP address * ⓘ
13.24.35.46

Next hop

Result
Next hop type
None

IP address
10.1.1.100

Route table ID
`/subscriptions/2301e3a0-8420-...`

A screenshot of a Microsoft Azure diagnostic tool. The interface is a form with several input fields and dropdown menus. At the top, there are fields for 'Subscription' (set to 'MSDN Platforms Subscription'), 'Resource group' (set to 'Demo'), 'Virtual machine' (set to 'vm01'), and 'Network interface' (set to 'vm01165'). Below these are fields for 'Source IP address' (set to '10.1.1.4') and 'Destination IP address' (set to '13.24.35.46'). A large blue button labeled 'Next hop' is centered below the source and destination fields. Under the heading 'Result', it shows 'Next hop type' as 'None'. Below that, the 'IP address' is listed as '10.1.1.100'. At the bottom, there is a field for 'Route table ID' containing the value '/subscriptions/2301e3a0-8420-...', followed by a small copy icon.

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

The screenshot shows the Azure Diagnostics - VPN Troubleshoot interface. At the top, there are three dropdown filters: 'Subscription' set to 'MSDN Platforms Subscription', 'Resource group' set to 'Demo', and 'Location' set to 'East US'. Below these filters, a section titled '*Storage account' displays the URL <https://samcteusvmdiagnostic.blob.core.windows.net/vpn>. A large 'greater than' symbol (>) is positioned to the right of this URL. The main area is a table listing troubleshooting jobs:

Name	Troubleshooting s...	Resource status	Resource Group	Location
vng01	Running	Succeeded	Demo	East US
cn01	-	Succeeded	Demo	East US

- 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.

Add packet capture

Subscription *

MSDN Platforms Subscription

Resource group *

Demo

Target virtual machine *

vm01

Packet capture name *

capture01

Capture configuration

The packet capture output file (.cap) can be stored in a storage account and/or on the target VM.

Storage account File Both

Storage accounts *

samcteusvmdiagnostic

Maximum bytes per packet ⓘ

default: 0 (entire packet)

Maximum bytes per session ⓘ

default: 1073741824

Time limit (seconds) ⓘ

default: 18000

+ Add filter)

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

The screenshot shows the 'Source' configuration section of the Azure Diagnostics tool. It includes fields for Subscription (MSDN Platforms Subscription), Resource group (Demo), Source type (Virtual machine), and a dropdown for the specific virtual machine (vm01). The 'Destination' section allows selecting a virtual machine or specifying manually, with 'Specify manually' selected and the IP address 13.24.35.46 entered. Under 'Probe Settings', TCP is selected as the protocol. The 'Destination port' is set to 3389. In the 'Advanced settings' section, the 'Source port' is also set to 3389. A 'Check' button is at the bottom.

Source

Subscription * ⓘ
MSDN Platforms Subscription

Resource group * ⓘ
Demo

Source type * ⓘ
Virtual machine

*Virtual machine
vm01

Destination

Select a virtual machine Specify manually

URI, FQDN or IPv4 * ⓘ
13.24.35.46

Probe Settings

Protocol ⓘ
 TCP ICMP

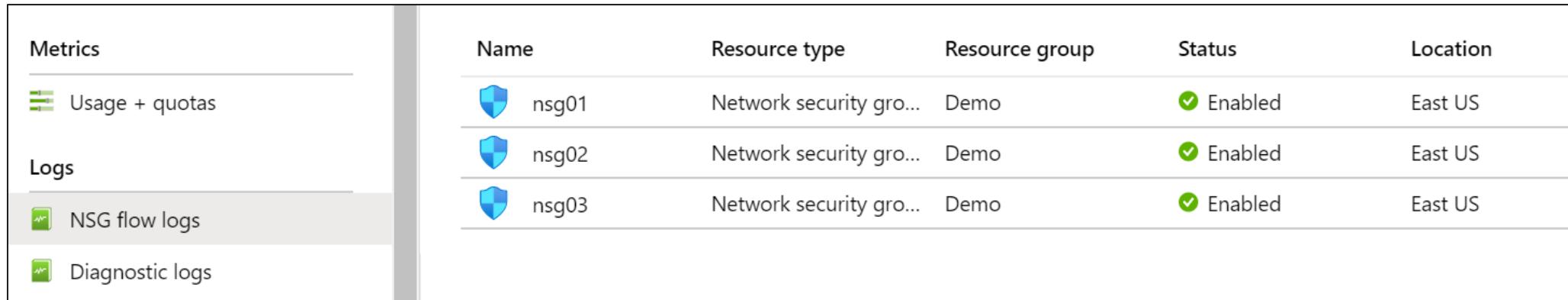
Destination port * ⓘ
3389

Advanced settings

Source port ⓘ
3389

Check

Logs - NSG Flow Logs

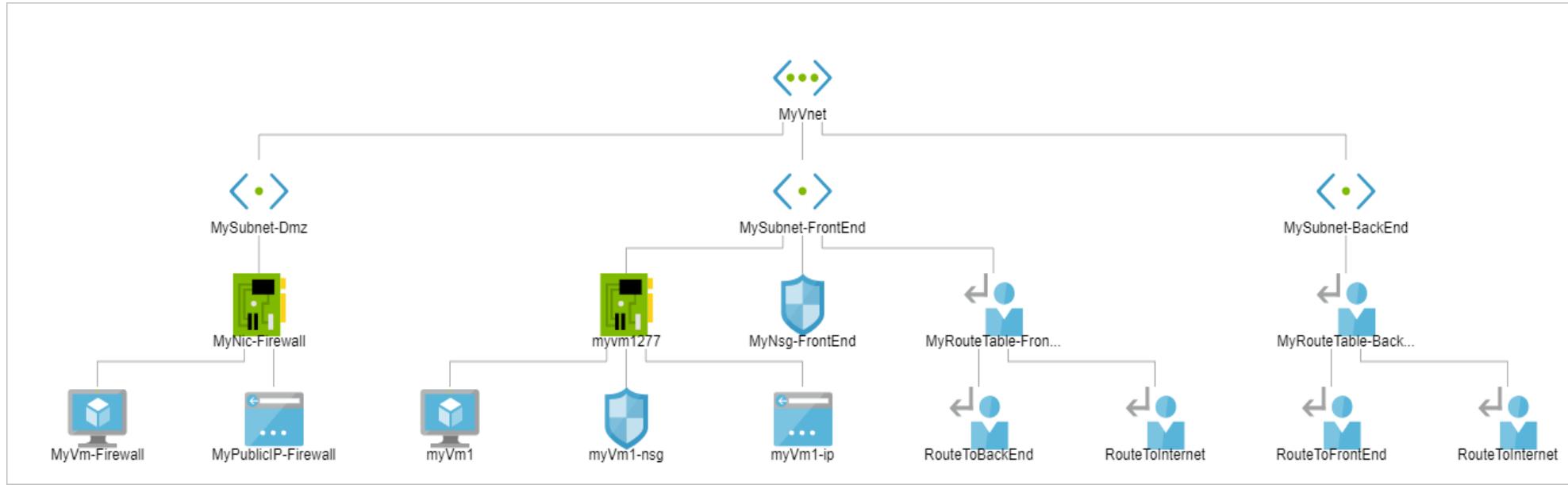


The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). On the left, there's a sidebar with options: Metrics, Usage + quotas, Logs (which is selected and highlighted in grey), NSG flow logs, and Diagnostic logs. The main area displays a table of NSG resources:

Name	Resource type	Resource group	Status	Location
nsg01	Network security gro...	Demo	Enabled	East US
nsg02	Network security gro...	Demo	Enabled	East US
nsg03	Network security gro...	Demo	Enabled	East US

- 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

Module 11 Lab and Review

