



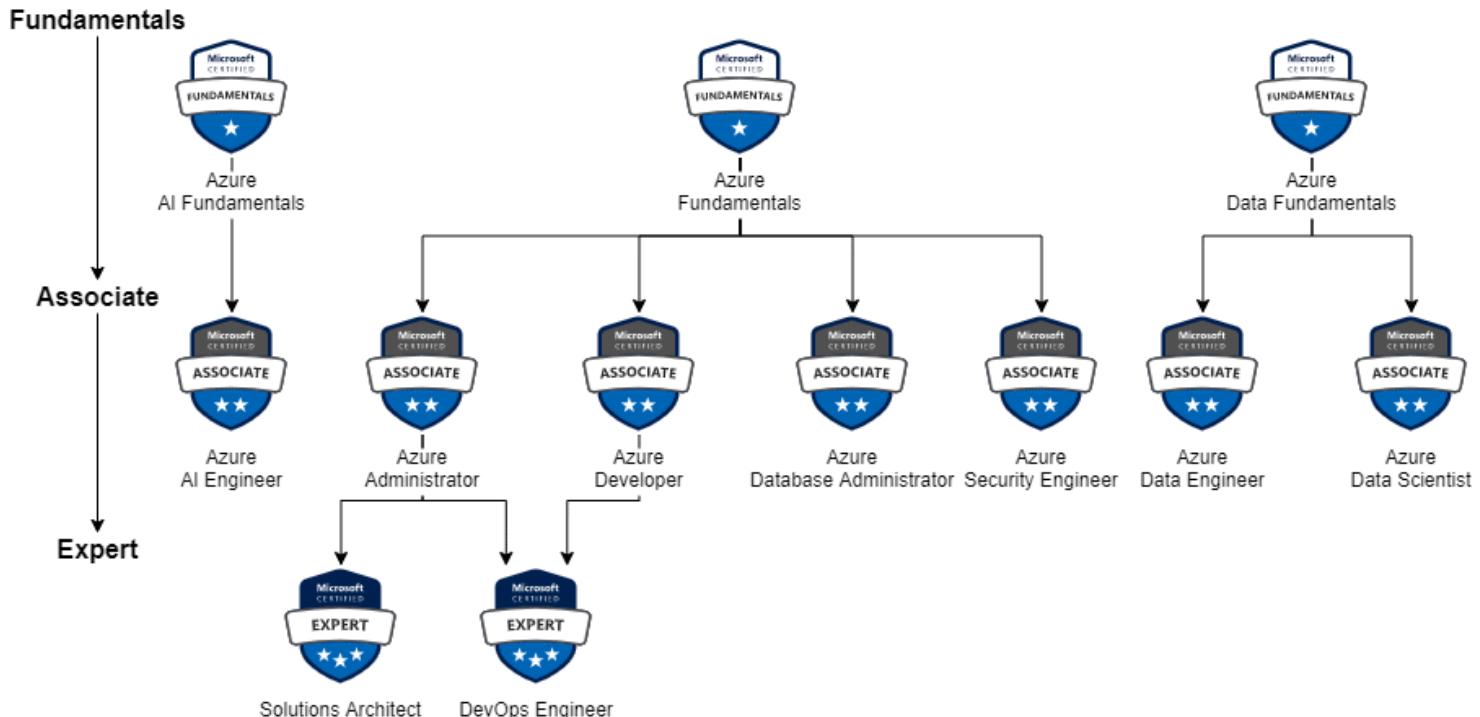
AZ-104

Microsoft Azure Administrator



AZ-104 Changes

28th July 2022





❖ Course Highlights

- ✓ Very detailed course, cover from basic to great details.
- ✓ Learn by doing approach
- ✓ Always updated with latest syllabus
- ✓ No shortcuts

❖ Approach:

- ✓ PPT/ concepts/ scenarios/ problems/ challenges/ solutions
- ✓ Learn by doing – lots of demos

❖ Prerequisite

- ✓ No prior certification required
- ✓ Recommended: 6+ months of hands-on experience



❖ Course Goal:

- ✓ Prepare you for AZ-104 certification
- ✓ Prepare you for a Azure Administrator job role
- ✓ Prepare you to have a solid foundation of Azure Cloud Computing

❖ What includes?

- ✓ 30+ hrs. of content, 100% syllabus covered
- ✓ Practice test, quizzes, notes, Imp links etc.
- ✓ PPT, Demo resources and other study material
- ✓ Full lifetime access
- ✓ Certificate of course completion
- ✓ 30-days Money-Back Guarantee

❖ Note:

- ✓ Captions are auto generated.
- ✓ Look at preview lessons before you purchase



LinkedIn



Saurabh Gupta

Microsoft Certified Trainer || CloudGita.com ||
Online Instructor || Azure
Microsoft | University of Maryland Global Campus

[View profile](#)

All

about me | resume | projects | interests | hobbies | contact



Microsoft

CloudGita.com

 **Rajdeep Sharma** • 2nd
Senior Analyst - Implementation
1d • Edited • 

+ Follow

View my verified achievement from [Microsoft](#).

Thanks to [Saurabh Gupta](#) for the wonderful course on Udemy !!

#microsoftazure #microsoft #cloudcomputing #growth #azure #training
#events #microsoftcertified #az900



Microsoft Certified: Azure Fundamentals was issued by Microsoft to Rajdeep Sharma.

[credly.com](https://credly.com/achievement/microsoft-azure-fundamentals) • 1 min read

 **Sourish Ghosh** • 2nd
Intern @Cognizant | Microsoft Azure Certified
2w • 

+ Follow • • •

Hey Everyone,

I am glad to share that I have successfully qualified Microsoft Azure AZ-900 certification.

Thanks to [Tata Consultancy Services](#) for giving this great opportunity to get Microsoft Certified.

Thanks to [RPS Consulting Pvt. Ltd.](#) for their support and guidance.

[Saurabh Gupta](#), your [Udemy](#) course helped me a lot to qualify in this certification exam.

#azure #microsoft #azurecloud #az900



AZ- 104 Exam Info

Everything you need to know



Exam Info

- ❖ **Exam Name:** AZ-104: Microsoft Azure Administrator
- ❖ **Exam official page:**
 - ❖ <https://docs.microsoft.com/en-us/certifications/azure-administrator/>
- ❖ **Cost:** 165 USD (India: ₹4800 INR - Price based on the country in which the exam is proctored)
- ❖ **Level:** Associate (not an easy exam)
 - ❖ We'll start from scratch and will cover everything you need to know to clear exam
- ❖ **Exam duration:** 180 minutes
- ❖ **No of Questions:** 45-65 questions
- ❖ **Question types:**
 - ❖ Multiple choice, and Multiple response
 - ❖ Drop down
 - ❖ Drag & Drop
 - ❖ Case studies
- ❖ **Passing Score:** 700/1000 (No negative marking)
- ❖ **Language:** English, Japanese, Chinese (Simplified), Korean, Spanish, German, French, Indonesian (Indonesia), Arabic (Saudi Arabia), Chinese (Traditional), Italian, Portuguese (Brazil), Russian
- ❖ **Retirement date:** 1 year

Udemy Tips

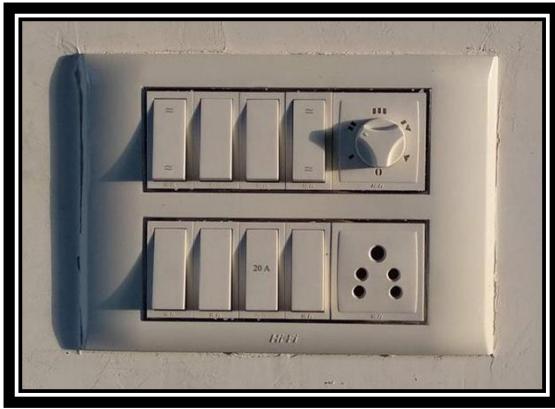
Udemy Tips

- ❖ Adjust your speed
- ❖ Transcript/Caption
- ❖ Video Quality
- ❖ Rating/Reviews is very important
- ❖ Udemy platform related issues - Please contact them directly
 - ❖ Udemy account
 - ❖ Billing
 - ❖ Site issues
 - ❖ Mobile app issues
 - ❖ Certificate of completion
 - ❖ Please contact Udemy support directly.

Why we need?

Cloud Computing

Why we need Cloud Computing?



Datacenter in the past



X Core
X GB Ram
X GB HDD

41 % Utilization

12 % Utilization

25 % Utilization

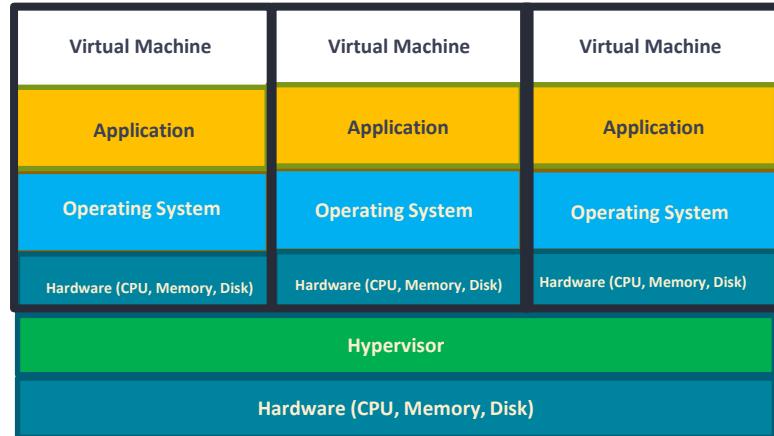
8 % Utilization

24 % Utilization

21 % Utilization

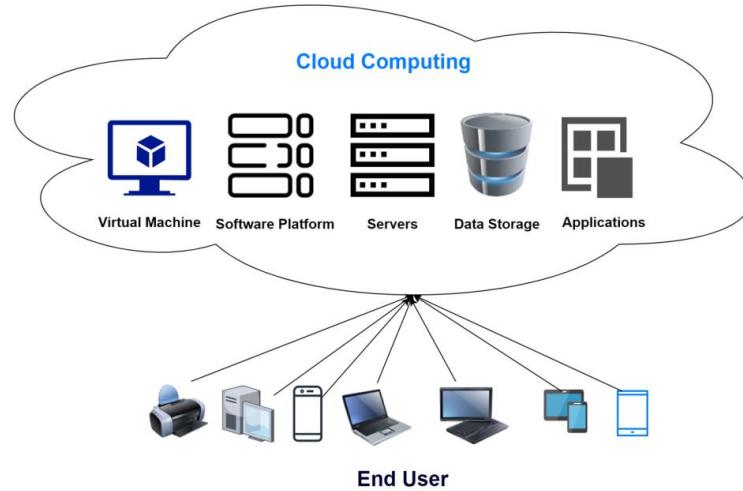
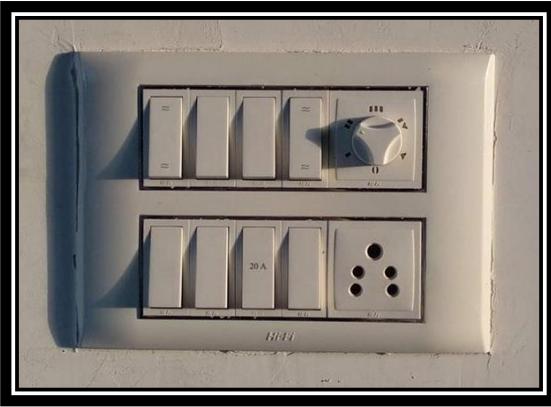
Virtualization

- High upfront cost
- Monthly expense even if not using
- Difficult to Scaling
- Maintenance



Virtualization

Introduction Cloud Computing



- Pay only what you use
- No plant maintenance
- Scaling

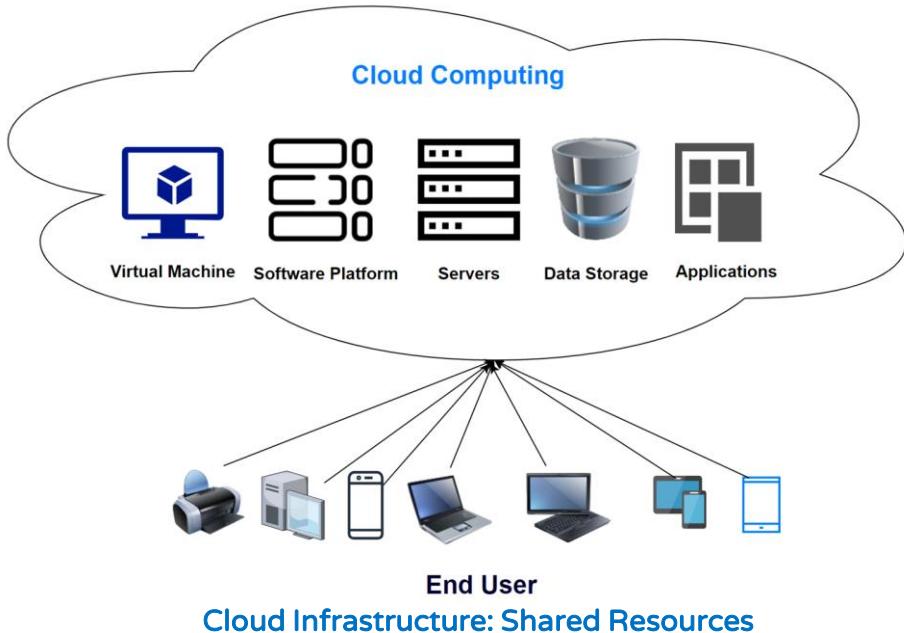
- Pay only what you use
- No Maintenance
- Scaling – Expand storage or compute power



Cloud Computing

What is Cloud Computing

- Cloud computing means Internet based Computing
- Renting IT Resources
- So, In simple terms, Cloud computing is on-demand resources delivered to you over the internet.
- Cloud Providers – Microsoft, AWS, Google
- Example – Gmail, Netflix, Dropbox
- Same resources shared by multiple clients





Set Budget

Set Budget and Delete Resources

- FREE Subscription
 - Azure won't charge you for your free subscription.
 - Your FREE subscription and services are disabled once your credit runs out.
 - You must upgrade to continue using Azure services.
- Paid subscription - **VERY IMPORTANT**
 - **DELETE RESOURCES AFTER YOUR USE/DEMO**
 - **EVEN IF I DON'T TELL YOU AFTER DEMO**
- Set Alert - notify you when your spending reaches or exceeds the amount defined in the alert condition of the budget.

Benefits of the cloud computing

New Startup



- Launching a new professional social network
- At launch, the focus will be on the United States.
- If the launch is a success, the company intends to expand globally.

Traditional Data Center Challenges



- Large up-front investment
- Forecast Infrastructure needs
- Took 5 months to setup there server
- Suddenly become popular
 - lot of users, experiencing latency
 - Scaling will need further few months of effort
 - Security and Compliance burden
- Less Load during off season
 - Now, difficult to scale down
 - Maintenance cost still going on
- Plan to Expand Globally
 - Same challenges again

Cloud Computing Benefits

Traditional Data Center Challenges

- Large up-front investment
- Forecast Infrastructure needs
- Took 5 months to setup there server
- Suddenly become popular
 - lot of users, experiencing latency
 - Scaling will need further few months of effort
 - Security and Compliance burden
- Less Load during off season
 - Now, difficult to scale down
 - Maintenance cost still going on
- Plan to Expand Globally
 - Same challenges again

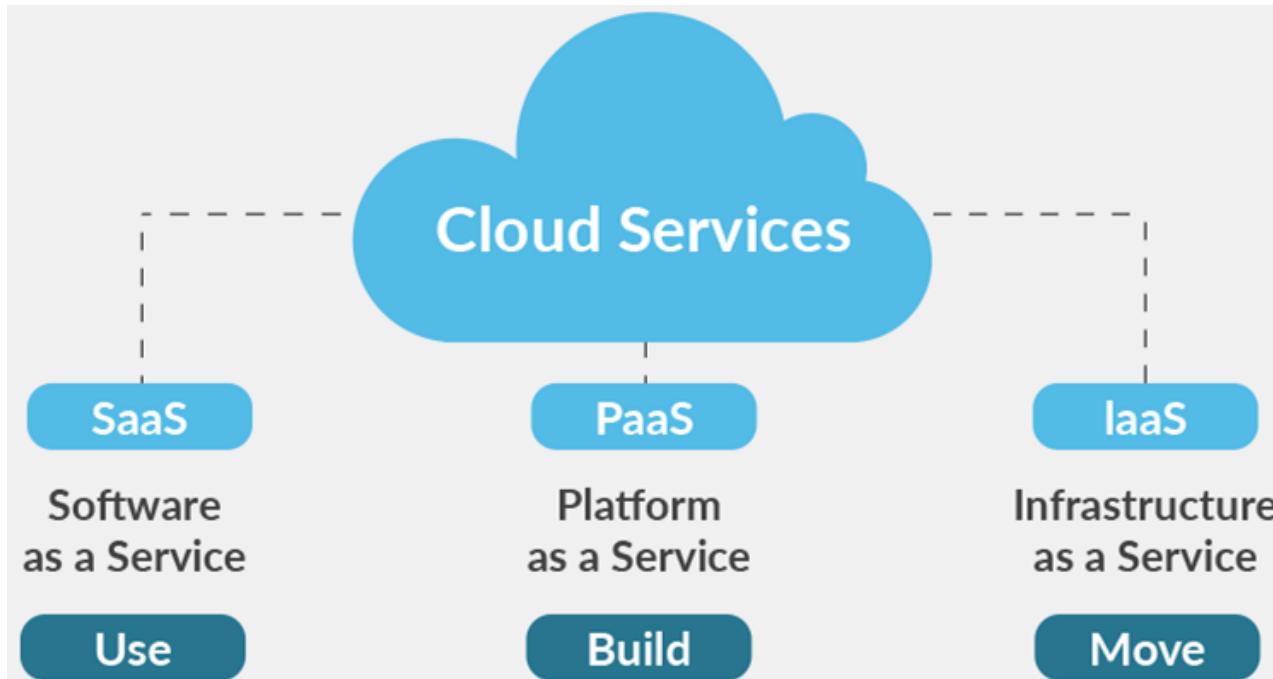
Advantages of Cloud Computing

- Trade capital expense for variable expense
 - No Initial investment
 - Pay only for how much you use – do not own hardware
- Stop guessing capacity
 - You can access as much or as little capacity as you need, and scale up or down in minutes.
- Increase speed and agility
 - New IT resources are only a click away
 - Reduce resource deployment time from weeks to minutes.
- Benefit from massive economies of scale
 - AWS can aggregate usage from hundreds of thousands of customers, they can lower pay-per-use prices.
- Stop spending money running and maintaining data centers
- Go global in minutes: In just a few clicks, you can easily deploy your application to multiple regions worldwide.

Computing Models

Categories of cloud services - SaaS vs PaaS vs IaaS

SaaS vs PaaS vs IaaS



SaaS vs PaaS vs Laas

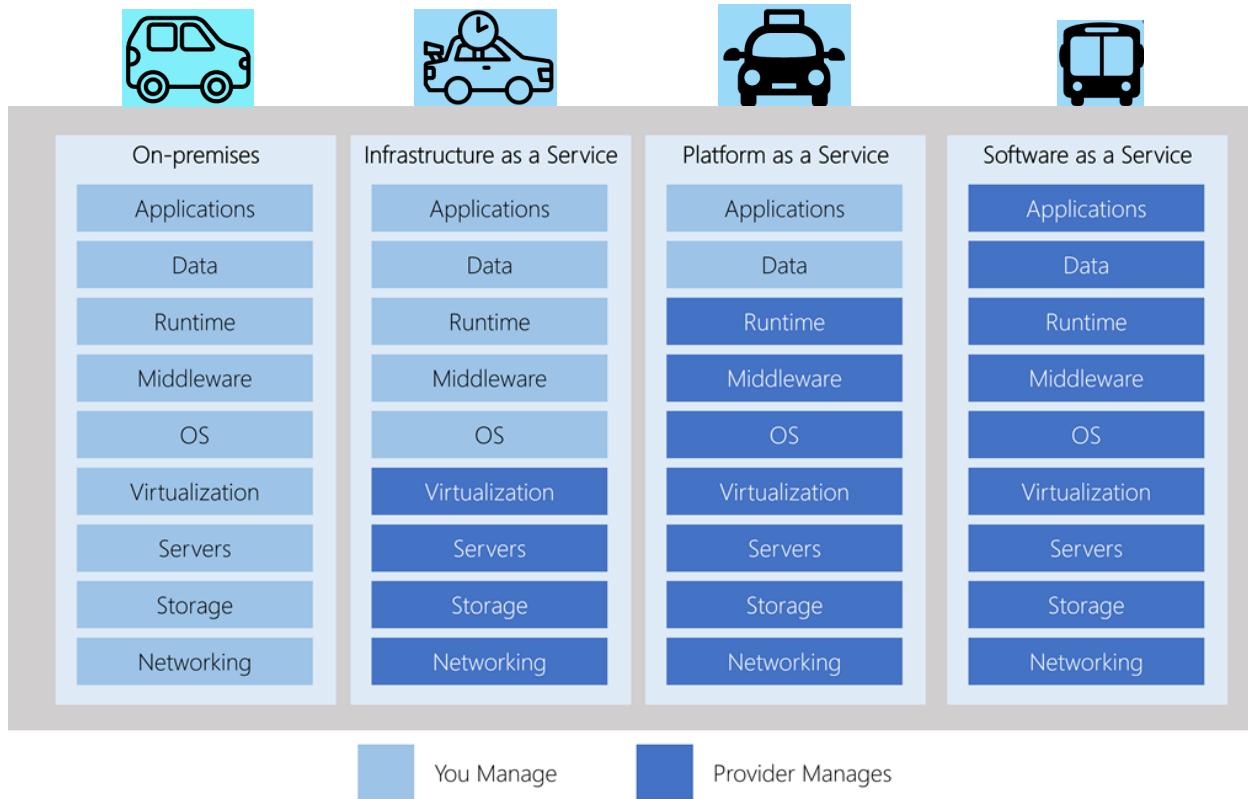


Your Own Car	Rental Car	Taxi/Uber	Bus
Navigation	Navigation	Navigation	Navigation
Vehicle	Vehicle	Vehicle	Vehicle
Driver	Driver	Driver	Driver
Insurance	Insurance	Insurance	Insurance
Fuel	Fuel	Fuel	Fuel
Maintenance	Maintenance	Maintenance	Maintenance
Upgrading	Upgrading	Upgrading	Upgrading

You Manage

Service Provider Manages

SaaS vs PaaS vs IaaS



SaaS vs PaaS vs IaaS

Cloud service model comparison

IaaS

The most flexible cloud service.

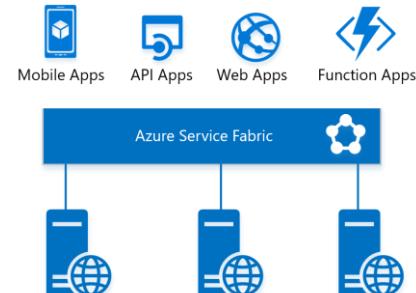
You configure and manage the hardware for your application.



PaaS

Focus on application development.

Platform management is handled by the cloud provider.



SaaS

Pay-as-you-go pricing model.

Users pay for the software they use on a subscription model.



Deployment Models

Types of Cloud Computing - Public, Private and Hybrid

Cloud Deployment Models



VS.

Hybrid Cloud

VS.



Private Cloud



Public Cloud



Public Cloud

- Cloud resources are those that are owned and managed by a third-party cloud service provider and are provided through the Internet.
- **Advantages**
 - No Maintenance
 - Near unlimited scalability
 - High reliability
- **Disadvantages**
 - Less control
- **Use case scenario**
 - Deploy website quickly
 - Focus on development



Private Cloud

- Cloud services that are utilized by a particular organization and are not accessible to the general public.
- **Advantages**
 - No Legal obligation
 - Control
 - Strict security and compliance
- **Disadvantages**
 - Infrastructure cost
 - Difficult to elasticity
 - IT Skills
- **Use case scenario**
 - Government policy requires specific data to be kept in-country



Hybrid Cloud

- Combination of public and private cloud with automation and orchestration between the two
- **Advantages:** Use your own equipment to meet security, compliance, or legacy scenarios
- **Disadvantages**
 - Expensive
 - Complicated
- **Use case scenario**
 - Medical data can't expose to public.
 - Application runs on old hardware.

Cloud Pricing Models

Factors that affect cost

Cloud Pricing Models

Traditional Data Center Cost

- Upfront Hardware cost
- Building, electricity, cooling, Internet
- Employees to maintain infrastructure
- Software/Application licenses
- And so on...

Cloud Computing Cost

- Can we save money?
 - Yes, but It's not straight forward
- Bill could depends on multiple metrics for each service
- Example: "Storage Service" pricing depends on:
 - Volume of data stored per month.
 - Quantity and types of operations performed
 - Data transfer costs.
 - Data redundancy/backups
- Example "VM" Pricing depends on:
 - Overall CPU time
 - Time spent with a public IP address
 - Incoming (ingress) and outgoing (egress) network traffic in and out of the VM
 - Disk size and amount of disk read and disk write operations

Cloud Pricing Models

Always FREE

- Virtual Network
- Azure Policy
- Azure Active Directory
- Azure Migrate
- Azure Open Datasets
- Azure Lighthouse
- Azure Private Link
- Azure Data Catalog
- Azure Service Fabric

Cloud Pricing Models

Pay: Time

- Charge based on time you use a particular service
- Other imp parameters like performance tiers and other configurations
- Examples:
 - Virtual Machine
 - App Services
 - SQL Database
 - Load Balancer

Cloud Pricing Models

Pay: GB

- Database Storage
- Storage Service
- Network traffic (between regions)

Cloud Pricing Models

Pay: Operations

- Charges based on number of operation
- Example: Cost per million operation
 - Storage services (read, write or delete operations)
 - Cosmos DB

Cloud Pricing Models

Pay: Execution

- Serverless offerings
- Charges only when you use, per execution
 - Azure Function
 - Serverless Database
 - Logic Apps

Cloud Pricing Models

Pay: Other metrics

- Example: Azure Active Directory Premium tier
 - Charge based on number of user licenses

Cloud Pricing Models

Other Parameters

- Regions/Locations
- How you purchase service
 - Through an Enterprise Agreement
 - Directly from the web
 - Through a Cloud Solution Provider
- Support options
- Programs and offers
- And so on....

Azure Global Infrastructure

Data Centers, Regions, Region pairs

Regions



- Region, which is a physical location around the world where we cluster data centers.
- Azure has more global regions than any other cloud provider.
- Better scalability and redundancy
- Preserve data residency
 - Low Latency
 - Global Footprint
 - High Availability
- How to choose region?
 - Compliance
 - Proximity
 - Available services
 - Pricing

Azure region pairs

- Each Azure region is always paired with another region within the same geography
- Data centers are usually 300+ miles apart
- Automatic replication and failover for some azure services.
- Additional advantages of region pairs:
 - If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure at least one is restored as quickly as possible for applications hosted in that region pair.
 - Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
 - Data continues to reside within the same geography as its pair.



Azure Global Infrastructure

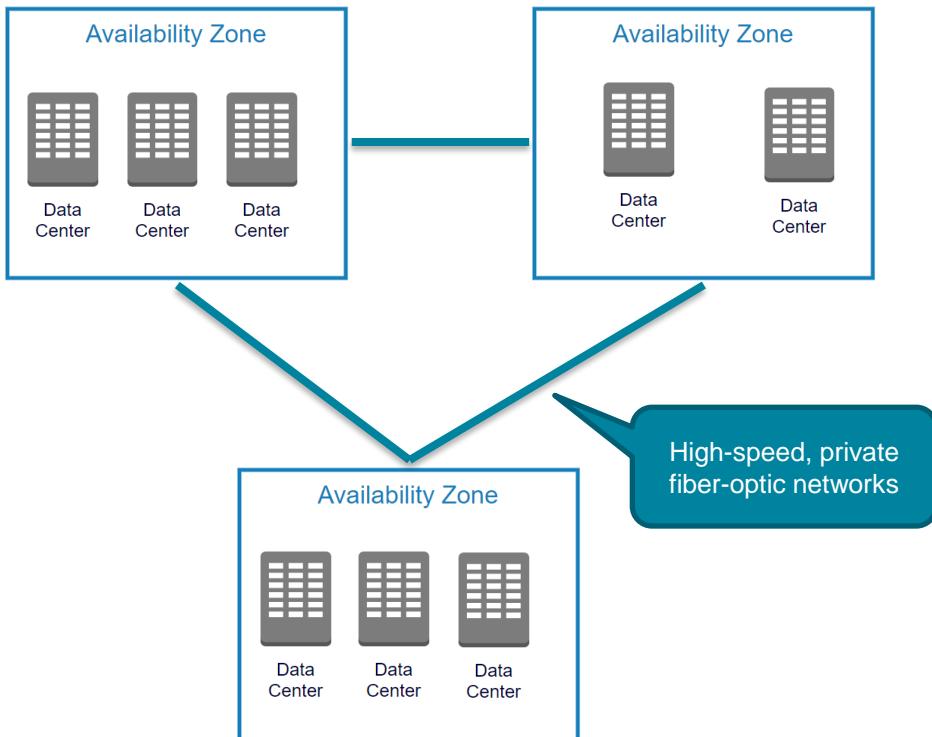
Availability Zones

Regions



Availability Zones

F Region

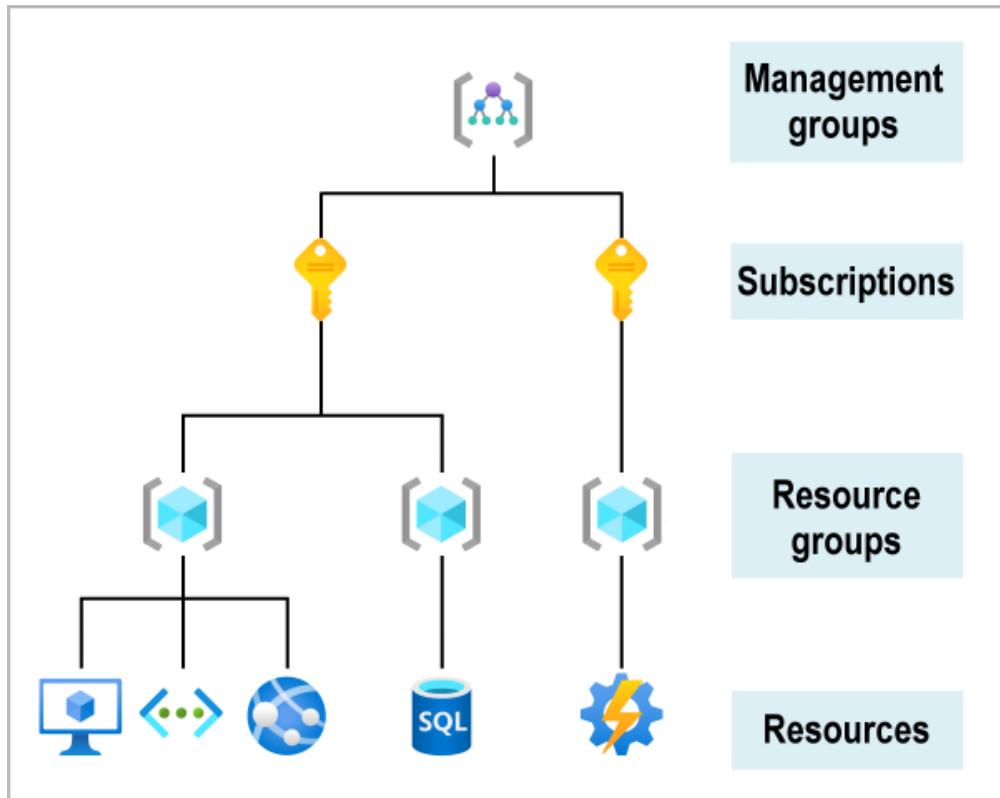


- Region represents a separate geographic area.
- Availability zone is a set of discrete data centers.
- Availability zone is set up to be an isolation boundary. If one zone goes down, the other continues working.
- Each availability zone has independent power, cooling and networking.
- Availability zones are connected via high bandwidth, ultra-low latency networking
- AZs are physically separated by several kilometers, while being within 100 km (60 miles) of one each.
- All AZ traffic is encrypted.
- Not every region has support for availability zones.

Resource Groups

Logical container for resources

Organizing structure for resources



- **Resources**: Resources are instances of services that you create, like virtual machines, storage, or SQL databases.
- **Resource groups**: Resources are combined into resource groups, which act as a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Subscriptions**: A subscription groups together user accounts and the resources that have been created by those user accounts. For each subscription, there are limits or quotas on the amount of resources that you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Management groups**: These groups help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.

Resource Groups

- Resources: are anything you create in an Azure subscription like VMs, Azure Application Gateway instances, and Azure Cosmos DB instances.
- Resource group is a logical container which help manage and organize your Azure resources.
 - For example similar usage, type, or location
- Each resource can exist in only one resource group.
- You can move a resource from one resource group to another group.
- Resource groups can't be nested.
- The resources in a resource group can be located in different regions than the resource group.
- Resource group created at location – to store metadata.
- A resource group can be used to scope access control for administrative actions. To manage a resource group, you can assign Azure Policies, Azure roles, or resource locks.
 - You can apply locks to a resource group or subscription to prevent deletion or make contained resources read-only. You can also apply locks directly to a resource.
- You can apply tags to a resource group. The resources in the resource group don't inherit those tags.
- Life cycle: When you delete a resource group, all resources in the resource group are also deleted.
- To create a resource group, you can use the portal, PowerShell, Azure CLI, or an ARM template.

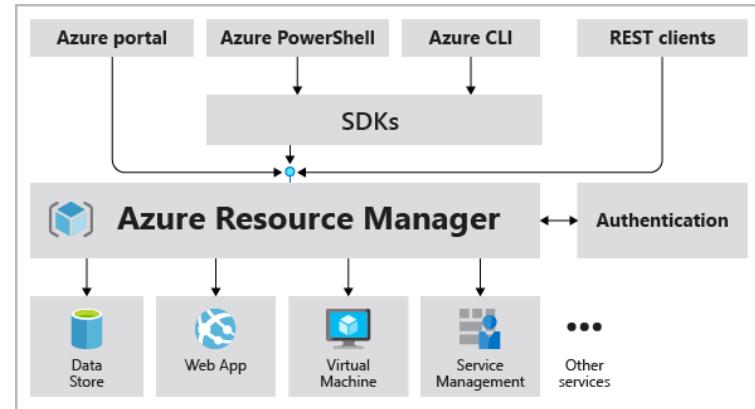


Azure Resource Manager

Deployment and management service for Azure

Azure Resource Manager (ARM)

- Automate resource deployments (create, update, and delete) using templates.
- ARM template is a JSON file that defines what you want to deploy to Azure.
- Integrates with Azure portal, PowerShell, CLI, and REST API to perform deployment and management tasks.
- Easy way to deploy multiple resource instances or reliably redeploy resources.
- ARM template can be used to deploy the resources consistently and repeatedly.
- Define the dependencies between resources so they're deployed in the correct order.

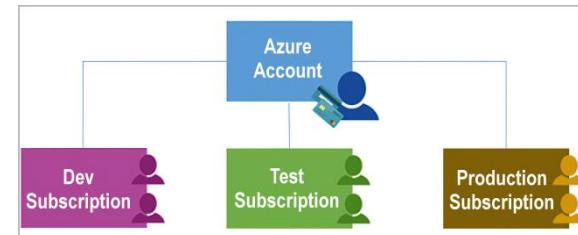


Subscription

How you are billed for resource usage

Subscriptions

- Using Azure requires an Azure subscription.
- An Azure subscription is a logical unit of Azure services that links to an Azure account. It also allows you to provision resources.
- A subscription provides you with authenticated and authorized access to Azure products and services.
- Azure generates separate billing reports and invoices for each subscription
- Two types of subscription boundaries
 - Billing boundary
 - Access control boundary
- You can create separate subscription based on:
 - Environment: development and testing, security, or to isolate data for compliance reasons
 - Organizational structures: IT, HR, Admin and so on
 - Billing: manage and track costs based on your needs, for example – Production, Test and Dev
- Different types of Subscription:
 - FREE: An email address and a credit card are required to sign up for a free trial subscription that provides \$200 credit for the first 30 days and 12 months of restricted access.
 - Pay-Per-Use: Charges monthly based on Cloud resource use.
 - Enterprise: A single Enterprise agreement is established for large subscription purchases, including savings for new licenses and Software Assurance.
 - Student: This membership includes \$100 for 12 months and may be activated without a credit card.

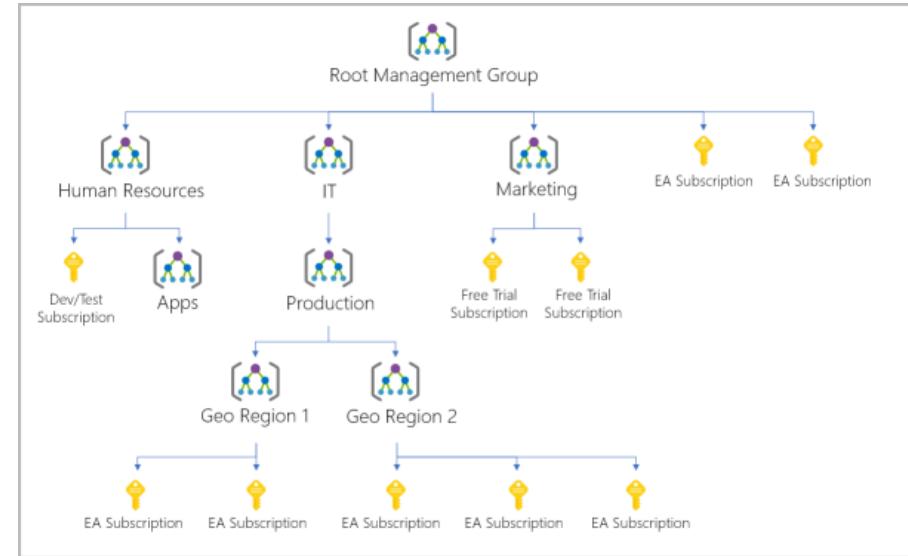


Management Groups

Organize multiple subscriptions as a single management entity

Management groups

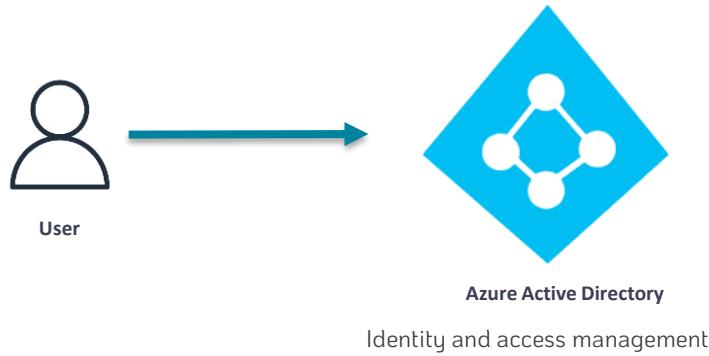
- Management groups let you organize multiple subscriptions as a single management entity to facilitate easier management.
- You can create management groups in a hierarchical structure with the top level of the hierarchy at the tenant level and containing all subscriptions in that tenant.
- Any conditions applied to a management group apply to all subscriptions contained in that management group object.
- Each management group and subscription can support only one parent.
- Each management group can have many children.
- The root management group can't be moved or deleted, unlike other management groups.



Azure Active Directory

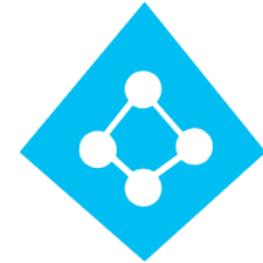
Microsoft's cloud-based identity and access management service

Azure Active Directory

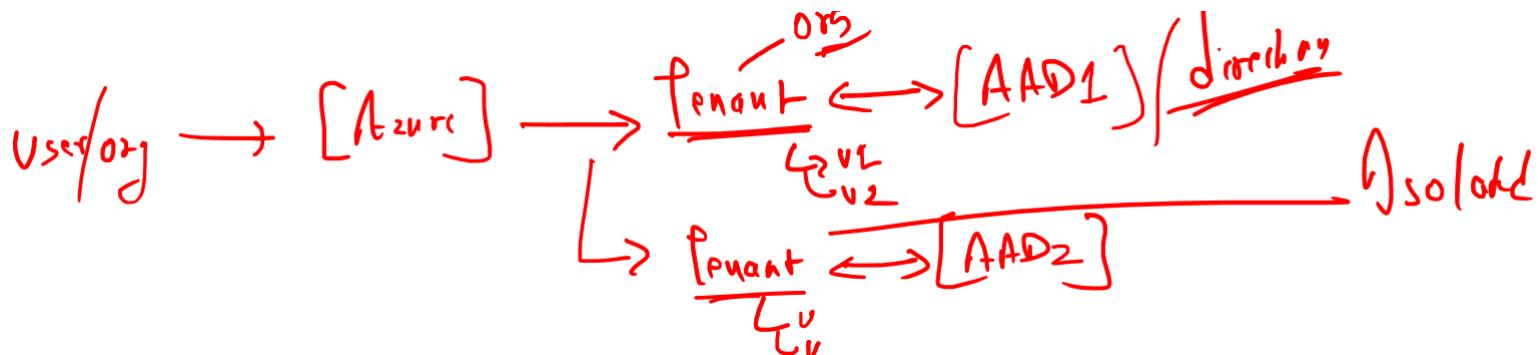


Azure Active Directory

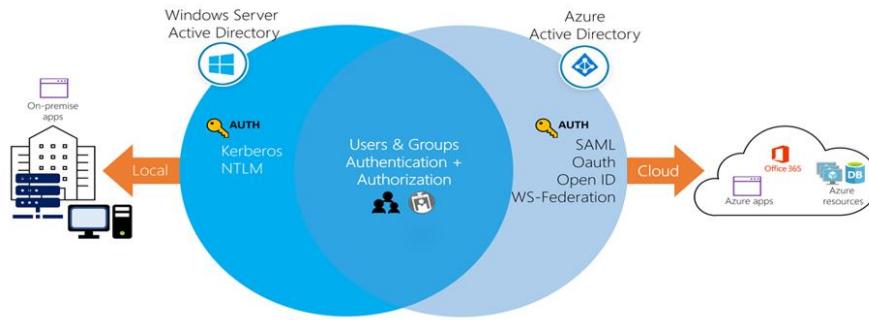
- Helps your employees sign in and access resources
- User information such as name, Id, email, password and address is stored in Azure AD by organizations.
- Identity: user or applications (require authentication via secret keys or certificates).
- Every day, Azure AD manages over 1.2 billion identities, according to Microsoft.
- Tenant
 - Represents an organization
 - Tenant is automatically created when your organization signs up for a Microsoft cloud service subscription.
 - The term Tenant means a single instance of Azure AD representing a single organization.
 - The terms Tenant and Directory are often used interchangeably.



Azure Active Directory

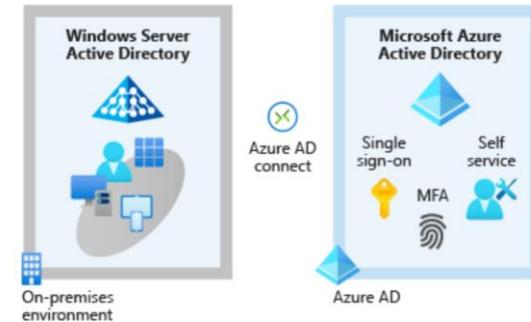


Windows Server AD (AD DS) vs Azure AD



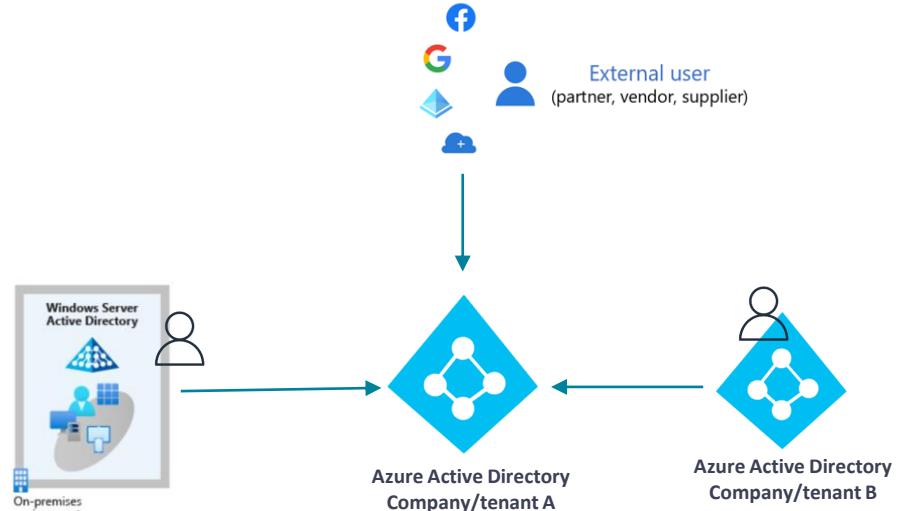
- **Windows Server AD:** Provides an identity and access management service that's managed by your own organization in **on-premises** environment.
- **Azure Active Directory:** cloud-based service
- **Communication Protocols:** Azure AD is HTTP/HTTPS based, it does not use Kerberos authentication.
 - Authentication - SAML, WS-Federation, and OpenID Connect
 - Authorization - OAuth

- Azure AD Connect **synchronizes user identities** between on-premises Active Directory and Azure AD.
- Azure AD provides extra features



User Accounts

- Cloud Identities
 - Users exists only in Azure AD
 - Local/your AAD or external AAD
- Guest Identities (External Identities)
 - B2B collaboration
- Directory-synchronized (Hybrid identities)

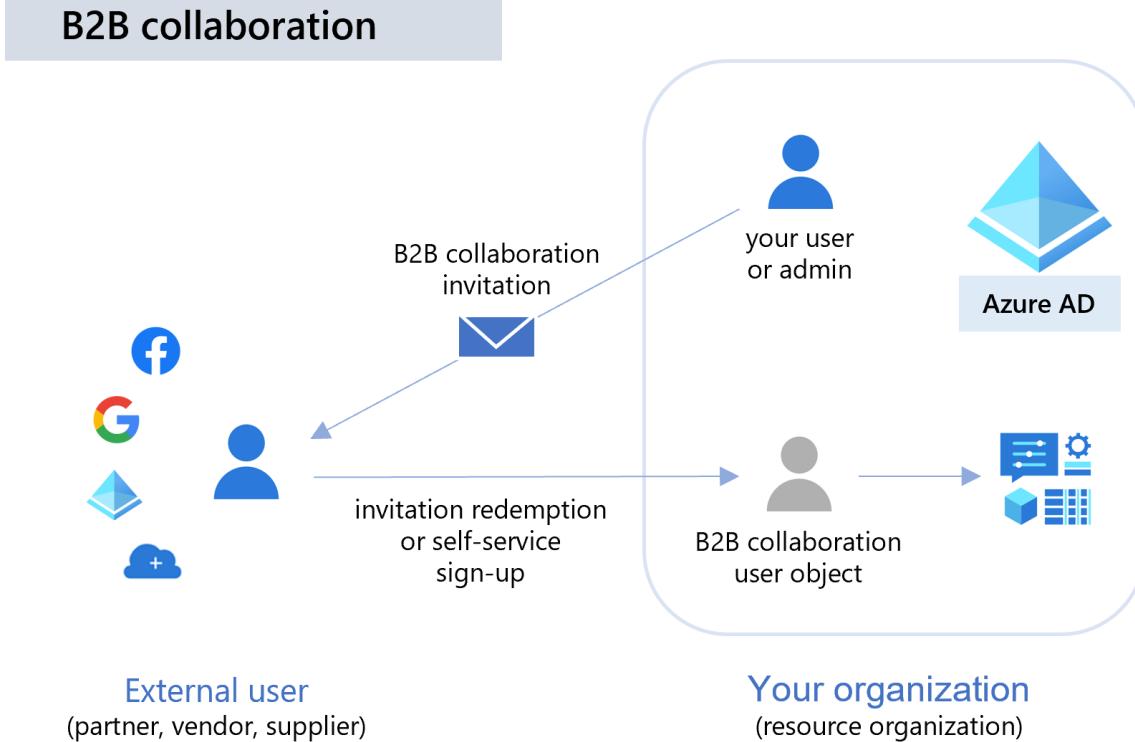


Users | All users

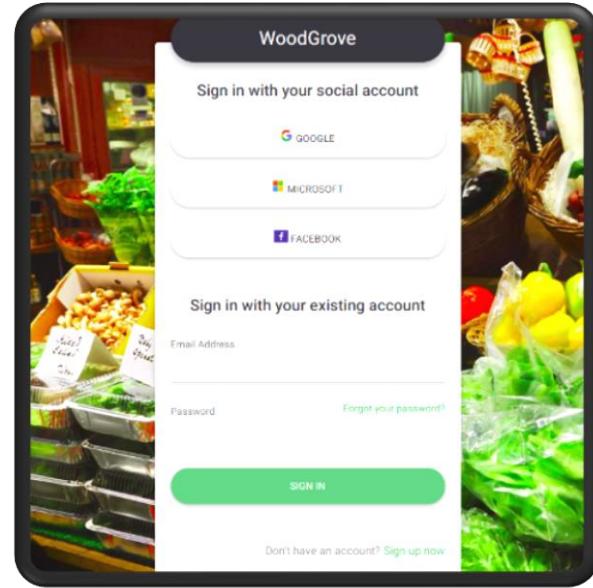
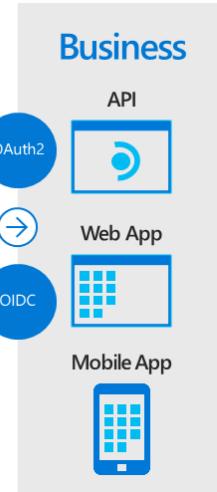
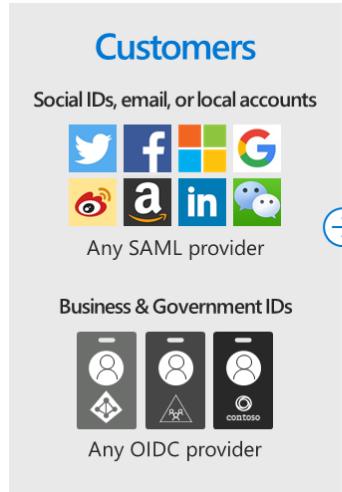
Microsoft - Azure Active Directory

All users	Name	User principal name	User type	Directory synced
Deleted users	C Retail Crisis Notifications	@microsoft.com	Member	Yes
Password reset	S [REDACTED]	@microsoft.onmicrosoft.com	Guest	No
User settings	R [REDACTED]	@microsoft.onmicrosoft.com	Guest	No
Diagnose and solve problems	-N [REDACTED]	@microsoft.onmicrosoft.com	Member	No

Azure B2B - External Users

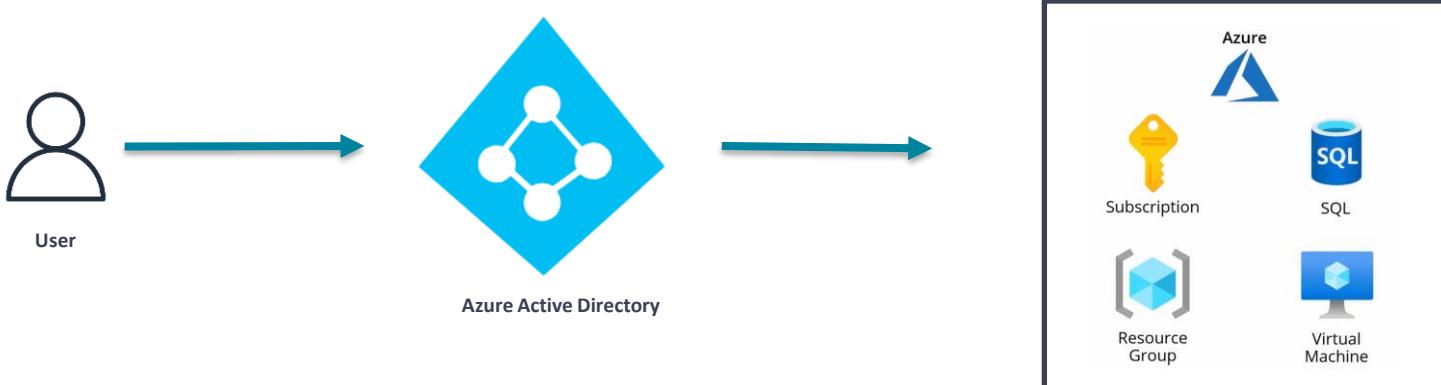


Azure B2C (business-to-customer)



- Azure AD B2C is a separate service from Azure Active Directory (Azure AD).
- It is built on the same technology as Azure AD but for a different purpose.
- It allows businesses to build customer facing applications, and then allow anyone to sign up into those applications with no restrictions on user account.

Azure AD Roles vs RBAC Roles



↑
Azure AD administrator roles

- Manage access to Azure Active Directory resources.
- Scope is at the tenant level.
- Examples:
 - Creating users/Groups/Roles
 - Managing Password
 - Billing/Payment Info

↑
RBAC Roles

- Manage access to Azure resources.
- Scope can be specified at multiple levels (management group, subscription, resource group, resource).
 - Create Database
 - Create/manage/delete VM and other resources

Administrative units

Azure AD administrator roles scope is at the tenant level.



Azure Active Directory



User Administrator

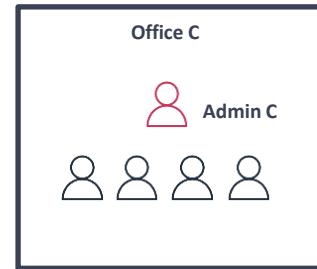
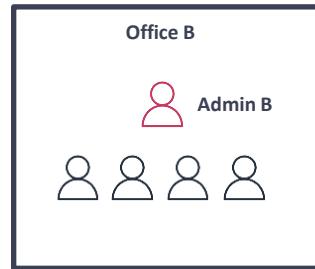
Administrative units



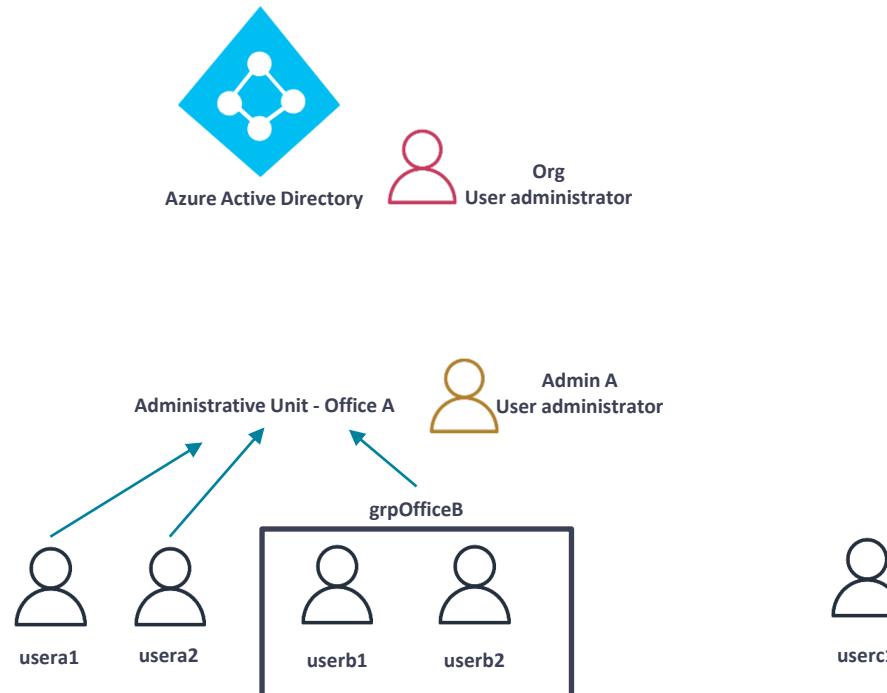
Azure Active Directory



User administrator

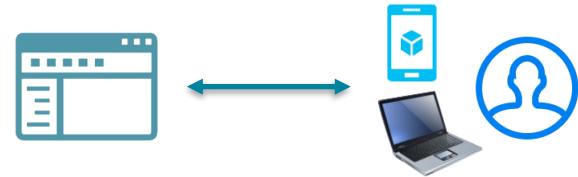


Administrative units



Azure AD Device Management

- Azure AD – Identity and access management service.
 - Identity – users, groups, applications or **devices**.
- Make sure devices are secure, compliant and not vulnerable.
- Capabilities: SSO, Conditional access

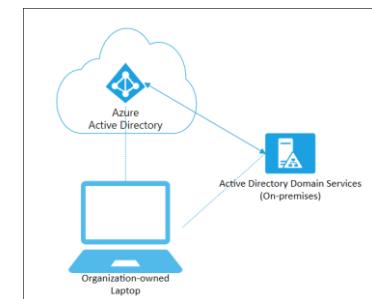
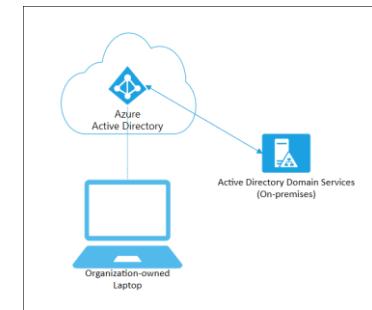
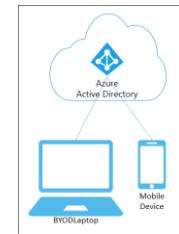


The screenshot displays the 'Devices' blade in the Microsoft Azure portal. The left sidebar includes links for 'All devices', 'Device settings', 'Enterprise State Roaming', 'BitLocker keys (Preview)', and 'Diagnose and solve problems'. The main area shows a table of 20 devices found, with columns for Name, Enabled, OS, Version, Join Type, Owner, MDM, and Compliant. The table lists various devices like 'TestAzureAD', 'AZDC03', and 'DESKTOP-614EKKI', along with their respective details. A search bar and filter options are also visible.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
TestAzureAD	No	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
AZDC03	No	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None	N/A
DESKTOP-614EKKI	No	Windows	10.0.19041.329	Azure AD joined	AzureAdmin	Microsoft Intune	No
vm-wvd-dj	No	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None	N/A
TestAzureAD	No	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
AzureADTestVM	Yes	Windows	10.0.17763.0	Azure AD joined	None	None	N/A
DESKTOP-C2SUE...	Yes	Windows	10.0.19043.844	Azure AD joined	AzureAdmin	Microsoft Intune	No
Home Desktop	No	Printer	v1.0	Azure AD joined	None	None	N/A
Home Desk	Yes	Printer	v1.0	Azure AD joined	None	None	N/A

Azure AD Device settings

- Azure AD registration
 - User-owned devices (BYOD)
 - Local user account to login in to device, corporate account to access resources
 - Limited management
 - Windows 10 or newer, iOS, Android, and macOS
 - Example: A user in your organization wants to access your benefits enrollment tool from their home PC.
- Azure AD join
 - Corporate-owned devices
 - Corporate user account
 - Full Intune management
 - Windows 11 and Windows 10 devices, Windows Server 2019 Virtual Machines running in Azure
 - Example: workers who work from home or are in remote branch offices with limited on-premises infrastructure.
- Hybrid Azure AD join
 - Suitable for hybrid organizations with existing on-premises AD infrastructure
 - Joined to on-premises AD and Azure AD requiring organizational account to sign in to the device
 - Gives you all the benefits of being cloud enabled, with still having full access to your on-prem infrastructure.



Multifactor authentication

Username
user@example.com

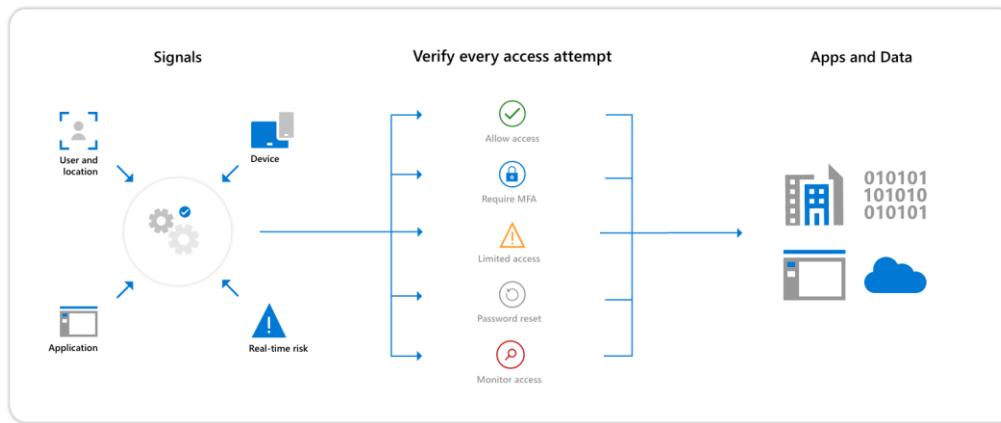
Password



- Two processes that enable secure authentication: Azure AD Multi-Factor Authentication and Conditional Access.
- Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate.
 - Something the user knows: This might be an email address and password.
 - Something the user has: This might be a code that's sent to the user's mobile phone.
 - Something the user is: This is typically some sort of biometric property, such as a fingerprint or face scan that's used on many mobile devices.
- Recommended for administrative accounts

Conditional Access

- Azure Active Directory uses Conditional Access to grant (or deny) resource access based on identity signals.
- Who the user is (Administrator or normal user)
- Where the user is (usual or unexpected location?)
- What device the user is requesting access from (is this a new device?)
- Based on signals AAD can decide to allow, deny, or require MFA access.
- Multi-authentication only if sign-in signals are unusual (like unexpected location)
- Need an Azure AD Premium P1 or P2 license



Source: Microsoft



Single sign-on (SSO)

- Problem statement - Why we need it?
 - Users had to create individual identity and password for each application
 - Difficult to remember credentials, and it's unsecure
 - When a user leaves an organization, finding all those identities and disabling them can be difficult.
- Single sign-on allows users to sign in once and access multiple resources and applications from multiple providers.
- With SSO, you need to remember only one ID and one password.
- As users change roles or leave an organization, access is tied to a single identity and so it is easy to manage.



Source: Microsoft

Azure RBAC

Role-based access control

Role-based access control

- Azure RBAC is system that allows control over who has access to which Azure resources, and what those people can do with those resources.
- Consists of three elements
 - Who has access to Azure resources?
 - Security principal - An identity that gets the permissions. It could be a user, group, or a service principal.
 - What they can do with those resources?
 - Role definition - A collection of permissions.
 - What is the Scope of access?
 - A way to constrain where those permissions are applicable.
- You can assign multiple Azure roles to a user account
- You can create your own custom Azure roles to assign custom permissions
- You can assign roles using the Azure portal, Azure CLI, Azure PowerShell, Azure SDKs, or REST APIs.

1

Security principal



	Role	Reader	Resource-specific	Custom	Contributor	Owner
Scope						
Management group	[User icon]					
Subscription	[Key icon]	Observers				Admins
Resource group	[Resource group icon]					
Resource	[Computer, Database, Blob icon]			Automated processes		

Role-based access control

Reader – Only view

Contributor – Read + Manage (update/delete)

Owner – Read + Manage + Grant

User Access Administrator – Manage user access

Deny Assignments

- Similar to windows deny files permission
- Blocks users from performing specific actions even if a role assignments allows it
- Can only be created using Azure Blue Prints or managed apps

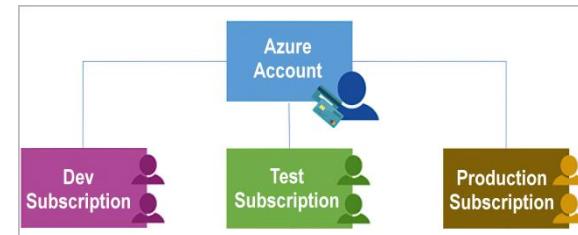
		Role				
		Reader	Resource-specific	Custom	Contributor	Owner
Management group	Reader	Observers	Users managing resources			Admins
Subscription	Reader	Observers	Users managing resources			Admins
Resource group	Reader	Observers	Users managing resources			Admins
Resource	Reader	Observers	Automated processes			Admins

Subscription

How you are billed for resource usage

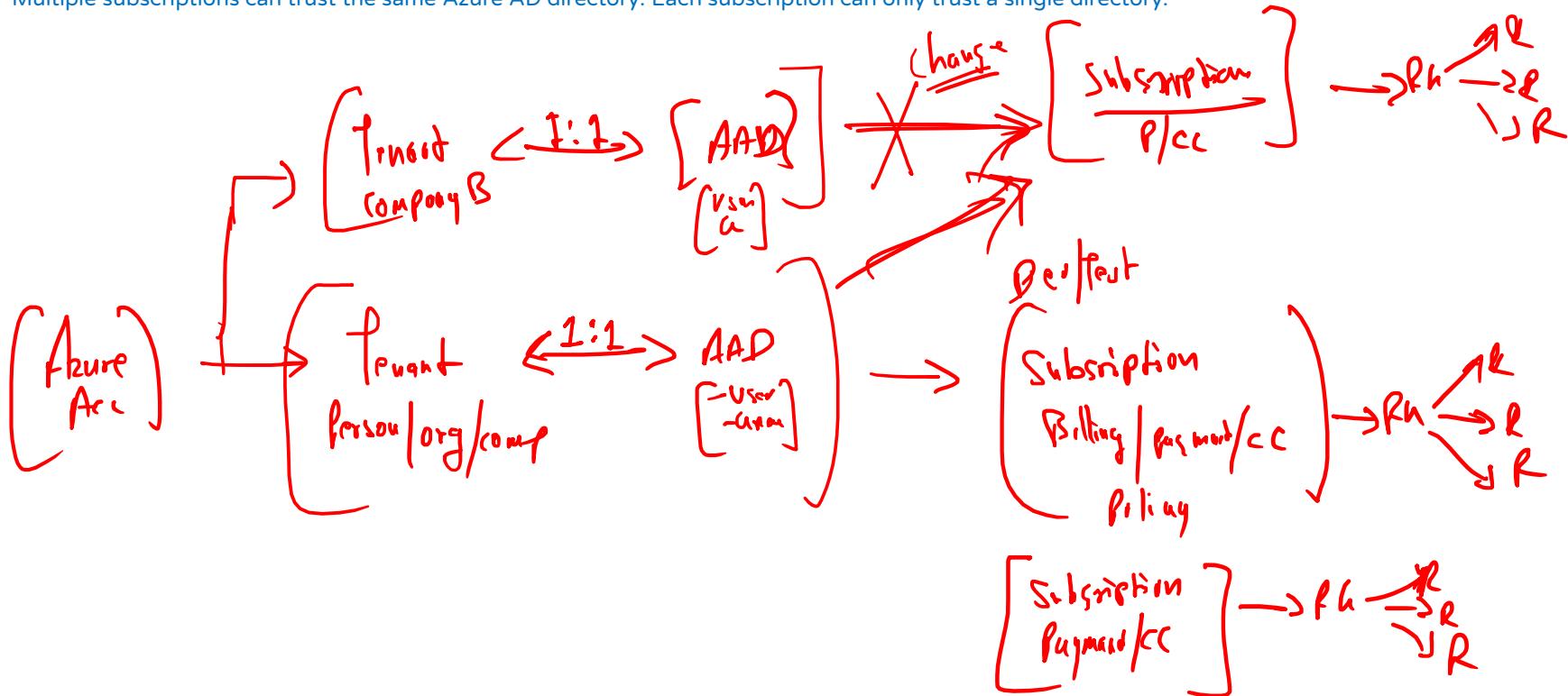
Subscriptions

- Using Azure requires an Azure subscription.
- An Azure subscription is a logical unit of Azure services that links to an Azure account. It also allows you to provision resources.
- A subscription provides you with authenticated and authorized access to Azure products and services.
- Azure generates separate billing reports and invoices for each subscription
- Two types of subscription boundaries
 - Billing boundary
 - Access control boundary
- You can create separate subscription based on:
 - Environment: development and testing, security, or to isolate data for compliance reasons
 - Organizational structures: IT, HR, Admin and so on
 - Billing: manage and track costs based on your needs, for example – Production, Test and Dev
- Different types of Subscription:
 - FREE: An email address and a credit card are required to sign up for a free trial subscription that provides \$200 credit for the first 30 days and 12 months of restricted access.
 - Pay-Per-Use: Charges monthly based on Cloud resource use.
 - Enterprise: A single Enterprise agreement is established for large subscription purchases, including savings for new licenses and Software Assurance.
 - Student: This membership includes \$100 for 12 months and may be activated without a credit card.

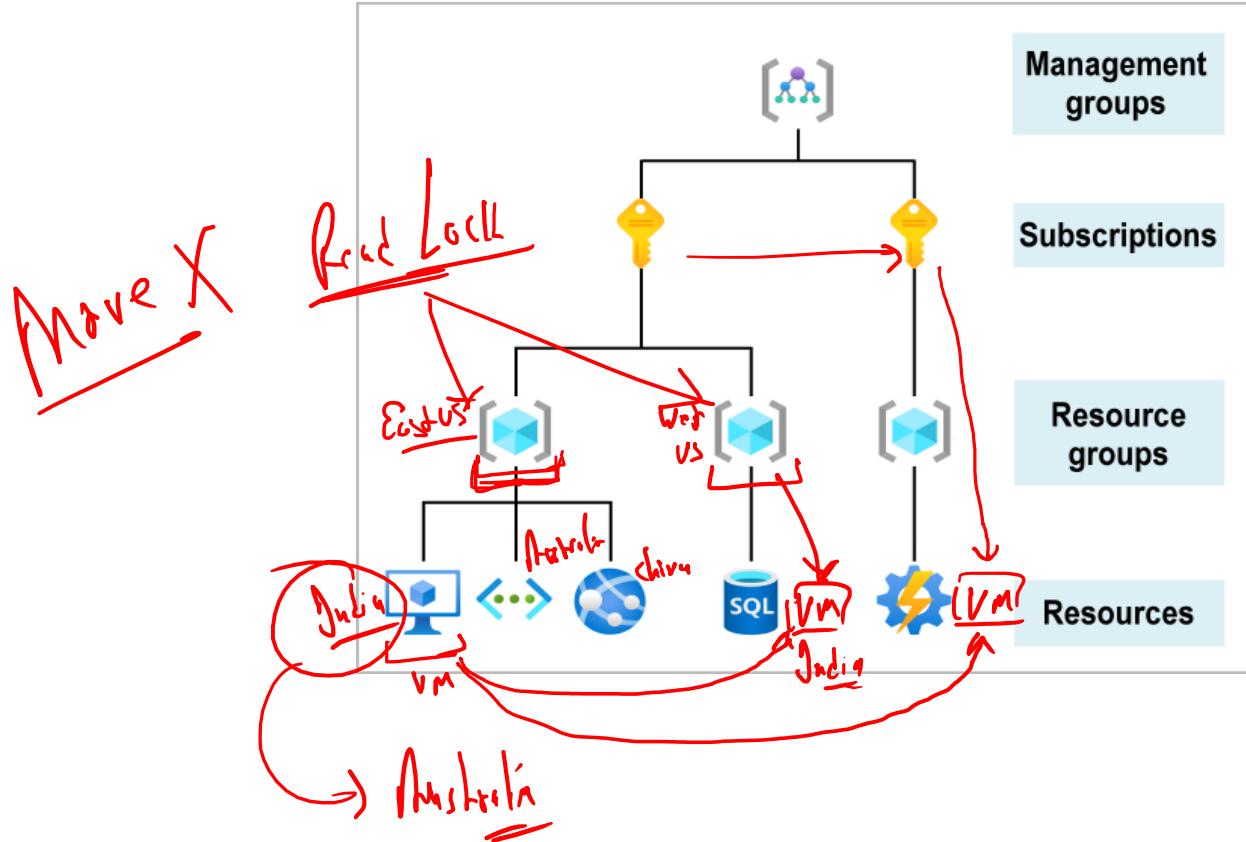


Trust Relation between AAD/Tenant and Subscription

- An Azure subscription has a trust relationship with Azure Active Directory (Azure AD).
- A subscription trusts Azure AD to authenticate users, services, and devices.
- Multiple subscriptions can trust the same Azure AD directory. Each subscription can only trust a single directory.



Move Resources between RG and Subscription



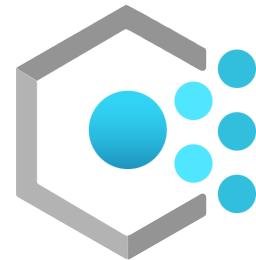
Azure Tags

- Azure tags are the name-value pairs that help to organize the Azure resources in the Azure portal.
- Azure Tags are simply labels that you can attach to your Azure resources.
- You can use tags to easily group and classify resources and assets in Azure.
 - For example, explore of the costs generated by resources having the same tag applied.
 - Tagging is a primary way to understand the data in any cost or billing reporting.
- Resources don't inherit any Azure tags applied at the Resource Group level.
- It's a fundamental part of any well-manage environment. It's also the first step in establishing proper governance of any environment.
- Azure Policy can be used to enforce tagging rules and conventions.
 - For example, you can require that certain tags be added to new resources as they are provisioned.



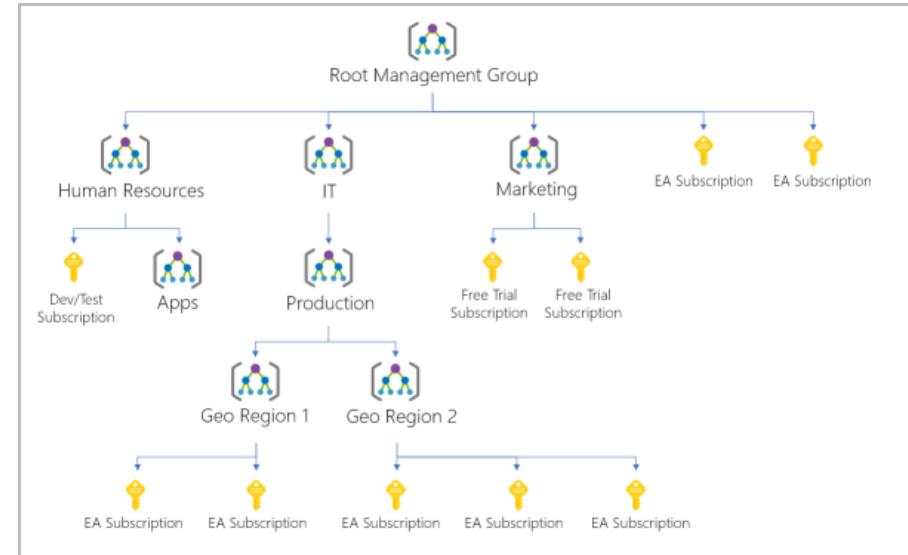
Azure Policy

- Azure Policy can help you control or restrict or audit your resources.
- Enforce rules on Azure resources configurations to make sure they remain compliant with corporate standards.
- You can apply individual policy or group of policy (initiatives).
- Two imp tasks
 - Prevent noncompliant resources from being created
 - Highlights existing resources that aren't compliant with the policies.
- Examples:
 - Allows only a certain SKU size for the virtual machines (VMs) to be provisioned.
 - Mandatory tags to be created while provisioning resources
 - MFA should be enabled on accounts with write permissions on your subscription
- Assign policy within a specific scope (management group, a single subscription, or a resource group.)
- Policy assignments are inherited by all child resources within that scope
 - You can exclude specific child resources you need to be exempt from the policy assignment
- You can review the noncompliant policy results and take any action that's needed.



Management groups

- Management groups let you organize multiple subscriptions as a single management entity to facilitate easier management.
- You can create management groups in a hierarchical structure with the top level of the hierarchy at the tenant level and containing all subscriptions in that tenant.
- Any conditions applied to a management group apply to all subscriptions contained in that management group object.
- Each management group and subscription can support only one parent.
- Each management group can have many children.
- The root management group can't be moved or deleted, unlike other management groups.



Cost Management

- This is a built-in service that gives you a breakdown of the usage and cost of your Azure resources.
- This allows you to see what is costing you money and how it compares against your budget.
- You use Cost Management + Billing features to:
 - Conduct billing administrative tasks such as paying your bill
 - Manage billing access to costs
 - Download cost and usage data that was used to generate your monthly invoice
 - Proactively apply data analysis to your costs
 - Set spending thresholds
 - Identify opportunities for workload changes that can optimize your spending



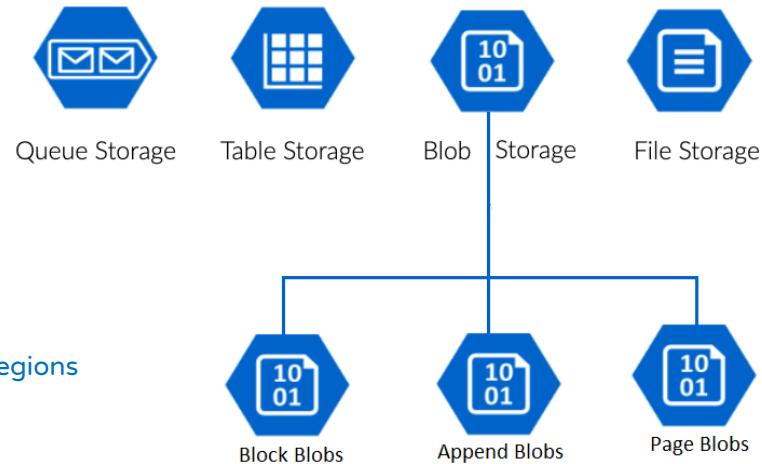
Source: Microsoft

Azure Storage Service

Fast, reliable, and private connection to Azure

Azure Storage Service

- Diff types of data and requirements
 - Relational, non-relational/No-SQL, datasheets, images, videos, backups
 - Storage, access, security, availability, latency, processing, backup
- Diff types of Data Service
 - Azure Blobs: Text and binary data
 - Azure Files: Managed file shares (SMB Protocol)
 - Azure Queues: Messaging
 - Azure Tables: NoSQL store
- Features
 - Durable and highly available – redundancy across datacenters or regions
 - Secure – all data encrypted by default
 - Scalable – massively scalable
 - Managed - Azure handles hardware maintenance, updates, and critical issues for you.
 - Accessible - accessible from anywhere in the world over HTTP or HTTPS.
 - Clients libraries are available in all languages
 - Support scripting in PowerShell or Azure CLI



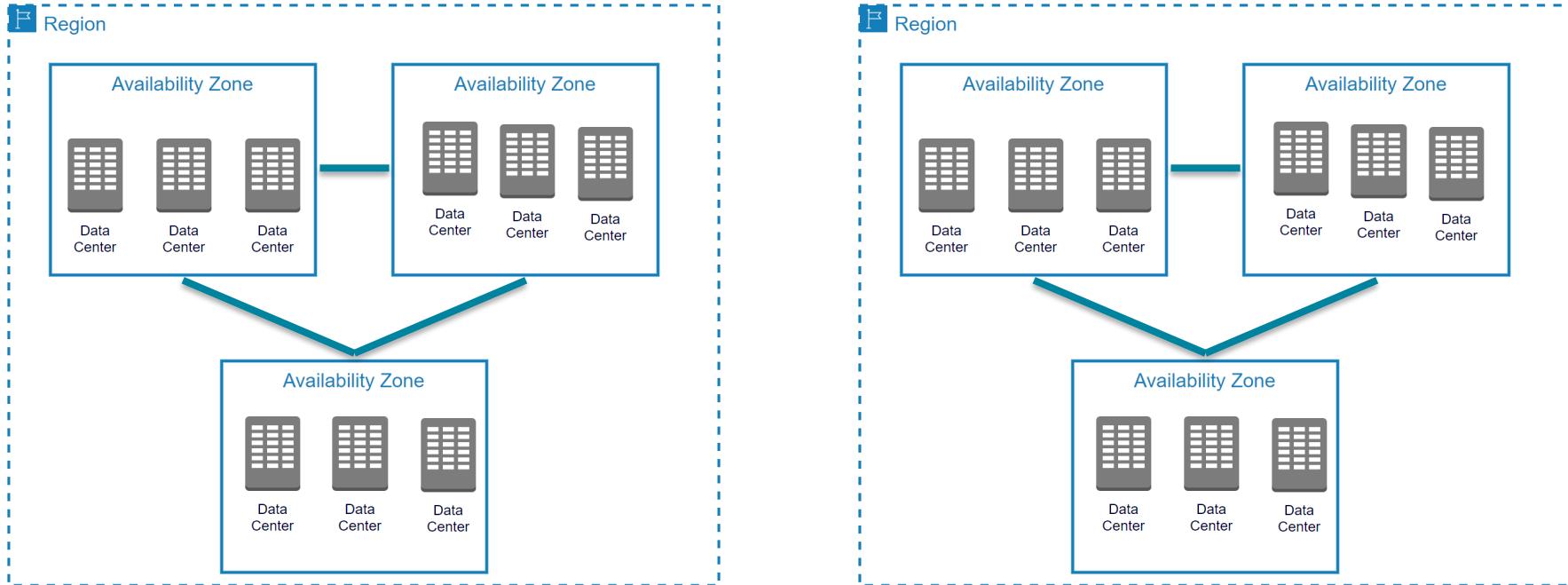
Azure Storage Data Redundancy

Protect your data from hardware failures, network or power outage, and natural disasters

Azure Data Redundancy

- Protect your data from hardware failures, network or power outages, and massive natural disasters.
- Even in the event of a failure, redundancy ensures your storage account's availability and durability.
- Tradeoffs between lower costs and higher availability
- Redundancy in the primary region
 - Locally redundant storage (LRS) – Three synchronous copies in same data center
 - Zone-redundant storage (ZRS) – Three synchronous copies in three availability zones (AZs)
- Redundancy in a secondary region
 - Geo-redundant storage (GRS) – LRS + Asynchronous copy to secondary region ()
 - Geo-zone-redundant storage (GZRS)
- With GRS or GZRS, the data in the secondary region isn't available for read or write access unless there is a failover to the secondary region.
- For read access to the secondary region, configure your storage account to use
 - Read-access geo-redundant storage (RA-GRS)
 - Read-access geo-zone-redundant storage (RA-GZRS).

Azure Storage Redundancy



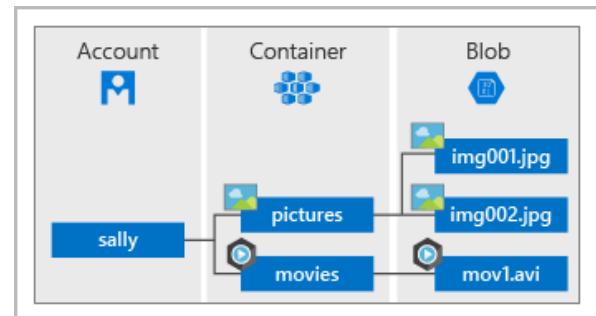
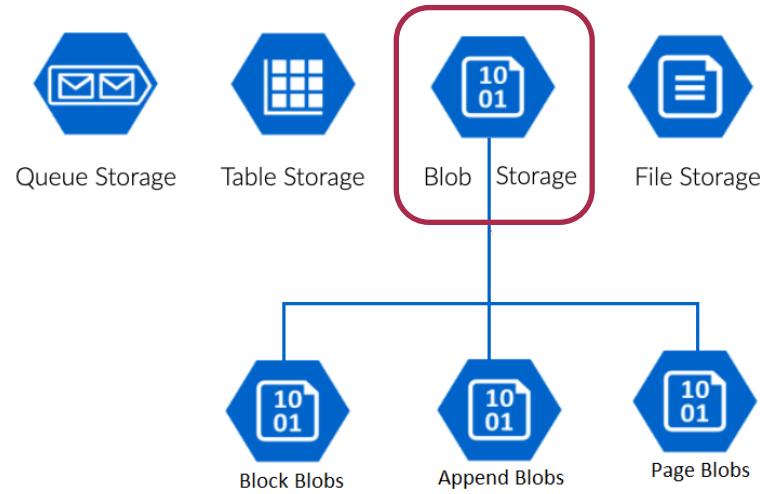
- Locally redundant storage (LRS) – Three synchronous copies in same data center
- Zone-redundant storage (ZRS) – Three synchronous copies in three availability zones (AZs)
- Geo-redundant storage (GRS) - LRS + Asynchronous copy to secondary region (three more copies using LRS) – Read only access
 - Read-access geo-redundant storage (RA-GRS) – Read Access on GRS
- Geo-zone-redundant storage (GZRS) – ZRS + Asynchronous copy to secondary region (three more copies using LRS) – Read only access
 - Read-access geo-zone-redundant storage (RA-GZRS) – Read Access on GZRS

Azure Blob Storage

Binary Large Object

Blob Storage

- **Blob - Binary Large Object**
 - Any type or format
 - Text, Images, audio, video, excel, backup files
- **Use cases:**
 - Storing files for shared access
 - Video and audio streaming
 - Storing data for analysis (Data Lake Gen2)
 - Writing to the log file
 - Storing data for disaster recovery, backup, and archiving
- Flat structure
- Provides a unique namespace in Azure for your data.
 - <http://mystorageaccount.blob.core.windows.net>



Three types of Blob Storage

➤ Block Blobs:

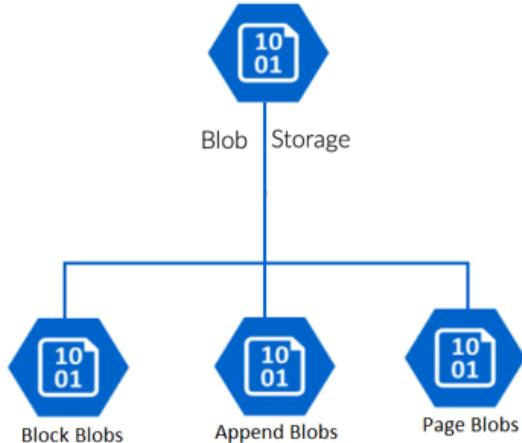
- For large objects that doesn't use random read and write operations, files that are read from beginning to end
- Such as media files or image files for websites.

➤ Page Blobs:

- Optimized for random read and write operations.
- Provide durable disks for Azure Virtual Machines (Azure VMs)

➤ Append Blobs:

- Optimized for append operations. e. g. Logs
- When you modify an append blob, blocks are added to the end of the blob only
- Updating or deleting of existing blocks is not supported
- For example, you might write all of your trace logging to the same append blob for an application running on multiple VMs

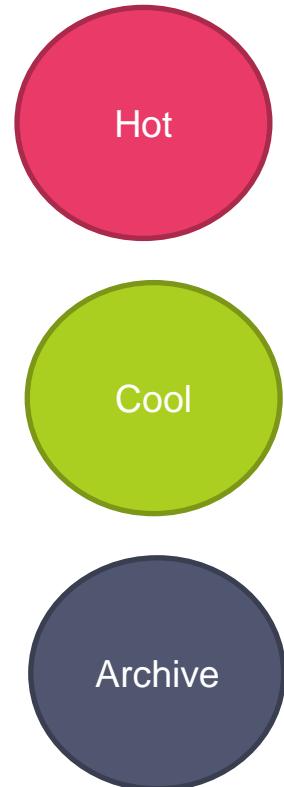


Storage Access Tiers

Organize your data based on attributes like frequency of access and planned retention period.

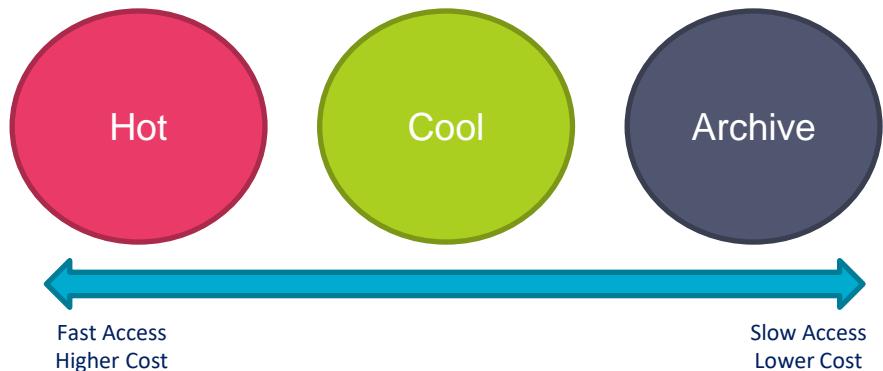
Storage Access Tiers

- Data stored in the cloud can be different based on how it's generated, processed, and accessed over its lifetime.
- Pricing
 - The volume of data stored/month
 - Types of operations performed
 - Number of operations performed
 - Data transfer cost, if any
 - The selected data redundancy option
- Organize your data based on attributes like frequency of access and planned retention period.
- Blob access tiers
 - Hot access tier
 - Cool access tier
 - Archive access tier



Storage Access Tiers

- **Hot**
 - Frequently accessed data
 - Example - images for your website
 - Low latency
 - Higher access cost
- **Cool**
 - Infrequent accessed data
 - Example - invoices for your customers
 - High latency
 - Lower cost
 - Stored for at least 30 days
- **Archive**
 - Rarely accessed data
 - Example - long-term backups
 - Highest access times and access cost
 - Latency in hours
 - Stored for at least 180 days
 - Use Case: Business policy mandated Data Archiving, long term retention like healthcare data



Performance Tiers

Standard

- Backed by magnetic drives
- Support – All storage account
- Optimized for high capacity and high throughput
- Provides the lowest cost per GB.
- Best for applications that require bulk storage or where data is accessed infrequently.
- Example: Backup and DR datasets, media, pictures, videos.

Premium

- Backed by solid state drives (SSD)
- Good for virtual machines and workloads that need low latency and high I/O performance
- Examples: transactional databases, big data analysis, IOT, AI or ML
- **Block Blob:** Best for high transaction rates or low storage latency
- **File Shares:** Best for enterprise or high performance applications that need to scale
- **Page blobs:** Best for random read and write operations

Note: You cannot change performance tier after account creation

Azure Table Storage

A NoSQL key-value store

Azure Table Storage

- NoSQL key-value Storage
- Items are referred to as rows, and fields are known as columns
- All rows in a table must have a key
- No concept of relationships, stored procedures, secondary indexes, or foreign keys
- Data will usually be denormalized
- To help ensure fast access, Azure Table Storage splits a table into partitions
- Support very large volume of Data
- Consider Cosmos DB for new development
- Advantages
 - It's simpler to scale
 - A table can hold semi-structured data
 - No complex relationships
 - Data insertion and retrieval is fast
- Good to use for:
 - Storing TBs of structured data capable of serving web scale applications
 - Storing datasets that don't require complex joins, foreign keys, or stored procedures, and that can be denormalized for fast access.
 - Capturing event logging and performance monitoring data.

	Key	Value (fields)		
	AA	Data for AA
	BB	Data for BB
	CC	Data for CC
	...			
	ZZ	Data for ZZ

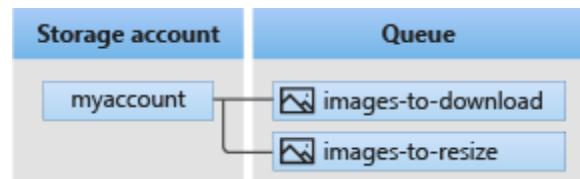
	Key (Customer ID)	Value (Customer Data)			
	C1	AAAAA	BBB	101 Block Street	YY 999 888
	C2	MM	NN	21 A Street	5 B Avenue
	C3	DDD	EEE	FFF	111 222 66 C Road

Azure Queue Storage

Message queuing service to store large numbers of messages.

Azure Queue Storage

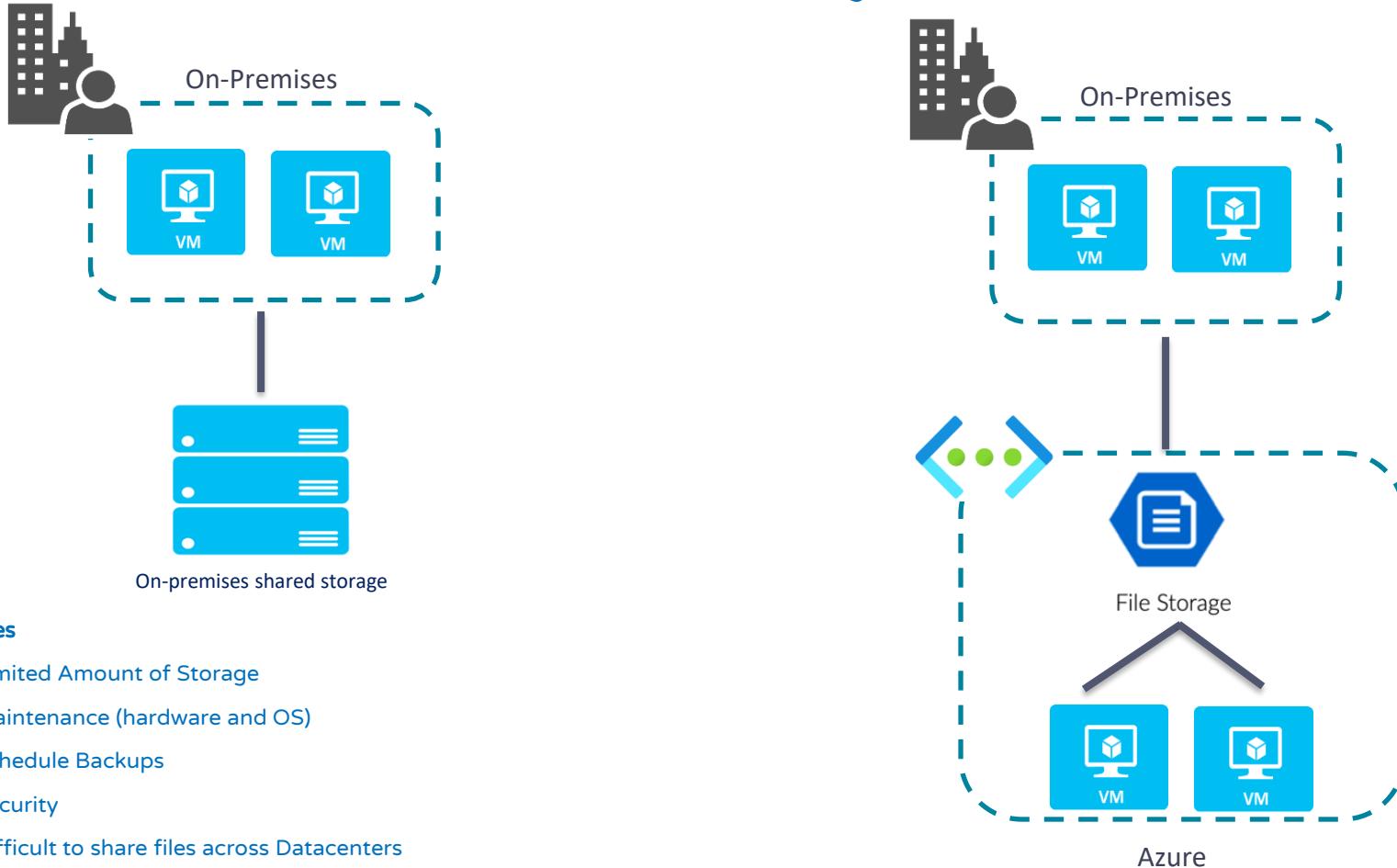
- Store large numbers of messages.
- Access messages via authenticated calls using HTTP or HTTPS.
- May contain millions of messages, up to the total capacity limit of a storage account.
- Queues are commonly used to create a backlog of work to process asynchronously.



Azure File Storage

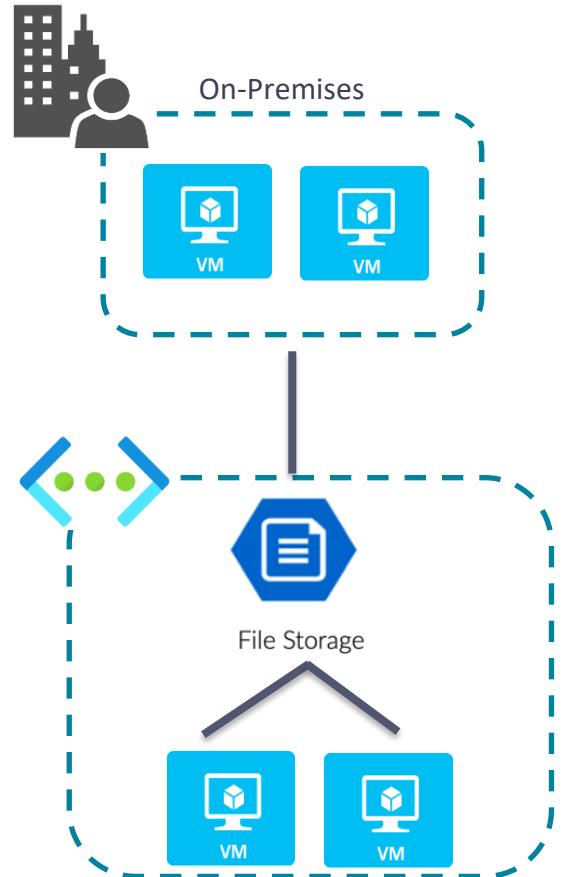
Simple, secure, and serverless enterprise-grade cloud file shares

Azure File Storage



Azure File Storage

- Enables you to create files shares in the cloud, and access these file shares from anywhere with an internet connection
- Mounted concurrently by cloud or on-premises deployments.
- Accessible from Windows, Linux, and macOS clients.
- Accessible Server Message Block (**SMB**) protocol or Network File System (**NFS**) protocol
- Azure Files ensures the data is encrypted at rest, and the SMB protocol ensures the data is encrypted in transit.
- **Use Cases**
 - Replace or supplement on-premises file servers
 - Share application settings
 - Dev/Test/Debug
- **Key Benefits**
 - Shared access: Replace on-premises file shares with Azure file shares without application compatibility issues
 - Fully managed: Azure will manage hardware or an OS
 - Resiliency: you don't have to deal with local power and network issues.



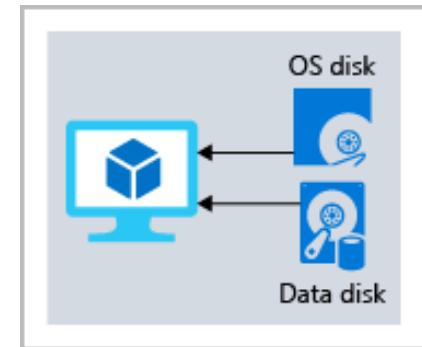
Disk Storage



High-performance, highly durable block storage for Azure Virtual Machines

Azure Disk Storage

- VM uses disks as a place to store an operating system, applications, and data in Azure.
- One virtual machine can have one OS disk and multiple Data disk but one data disk can only be link with one VM.
- Both the OS disk and the data disk are virtual hard disks (VHDs) stored in an Azure storage account.
- The VHDs used in Azure is .vhd files stored as page blobs in a standard or premium storage account in Azure.
- **Unmanaged disks:** We can create a storage account and specify it when we create the disk.
 - Not recommended, previous unmanaged disks should migrate to managed disk
- **Managed disk**
 - Azure creates and manages storage accounts in the background.
 - We don't have to worry about scalability issues.
 - Azure creates and manages the disk for us based on the size and performance tier we specify.
- **Managed Disk types:**
 - Standard HDD: Backup, non-critical, infrequent access
 - Standard SSD: lightly used production applications or dev/test environments
 - Premium SSD disks: Super fast and high performance, very low latency, recommended for production and performance sensitive workloads
 - Ultra disks (SSD): for most demanding IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads



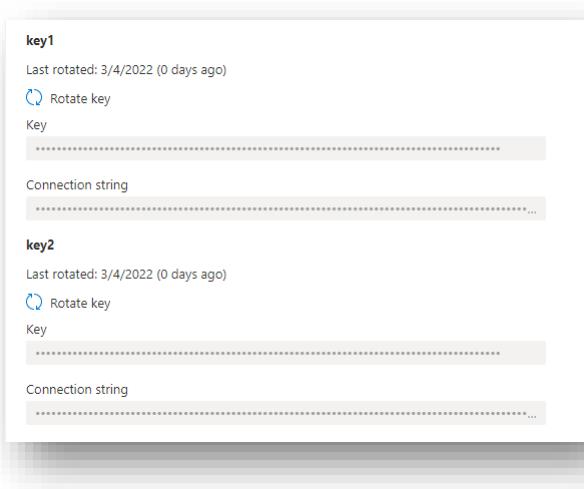
Data Storage Authorization

- Anonymous
 - Public access, no authorization is required
 - Use Case: Website, online documentation
 - Only for Blob
- Shared Key authorization
 - Data can be accessed using access keys
- Shared Access Signatures (SAS)
 - Provide limited delegated access
 - Constraints: time interval, permissions
- Azure Active Directory
 - Role-based access control - Fine-grained access can be provided to users, groups, or applications

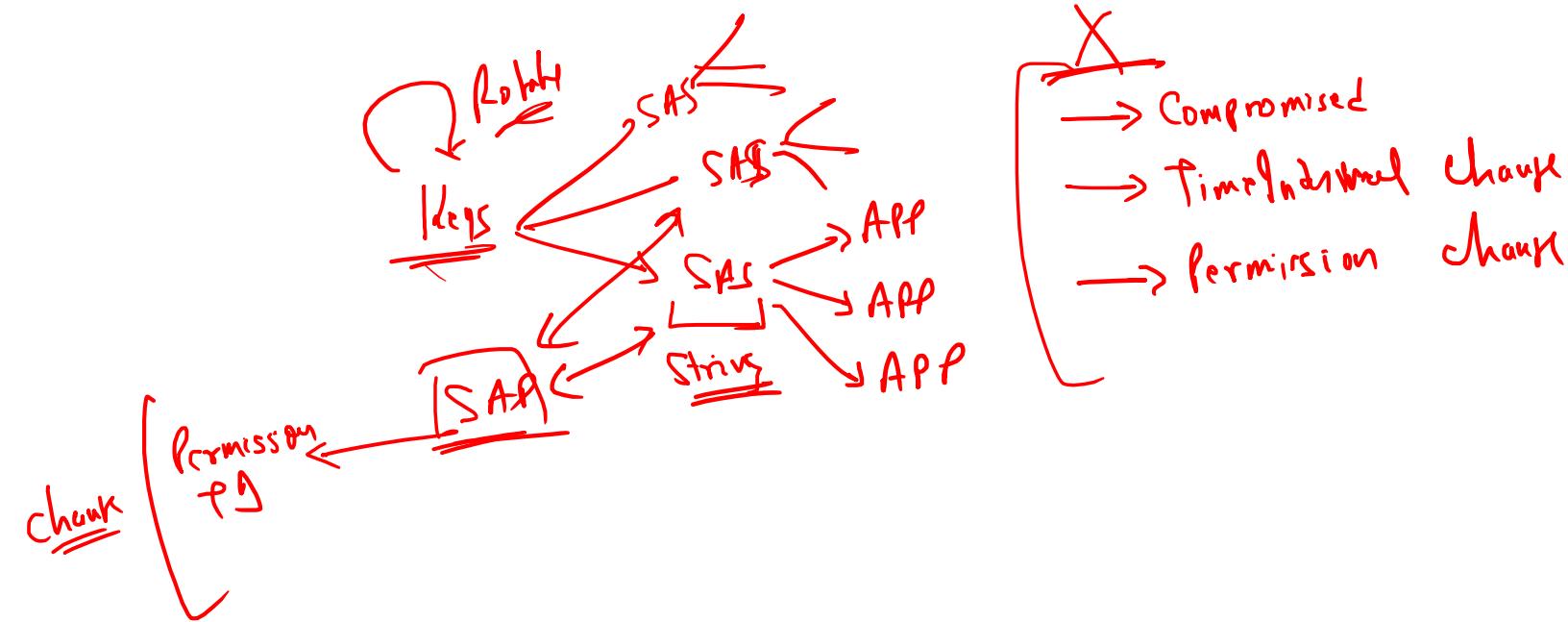


Shared Access Keys Authorization

- Two default access keys are generated with every storage account
- Whoever has these keys, can access entire storage account
- Make sure they're safe by not storing or hard coding them in your application code.
 - Store these on key vault
- If keys compromised, you can regenerate keys
- Recommendation: periodically rotate the keys
- Consider Azure AD instead



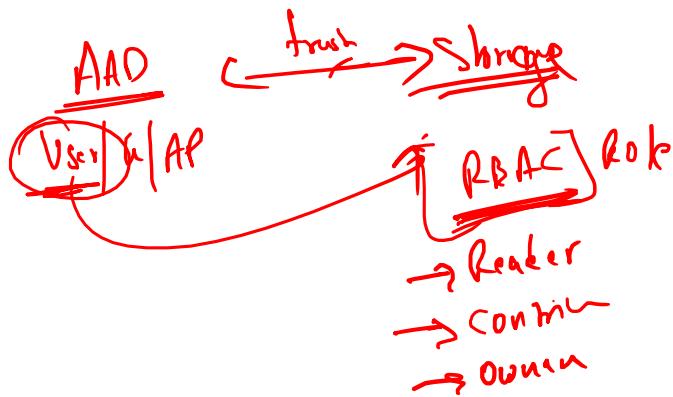
Stored access policies



- A stored access policy is a set of constraints that can be used by multiple shared access signatures.
- Contains permission and time interval
- Only work with service level shared access signature

Azure AD Authorization

- Azure storage can use Azure AD to authorize requests
- Storage Account level or service level (currently Blob and Queue only)
- Use Role-based access control (RBAC)
 - User, group or service principle
- Microsoft recommended approach.
 - Benefit: No longer need to store credentials within application config files
 - More secure, easy to implement and manage
- Similar to IIS application pool identity approach

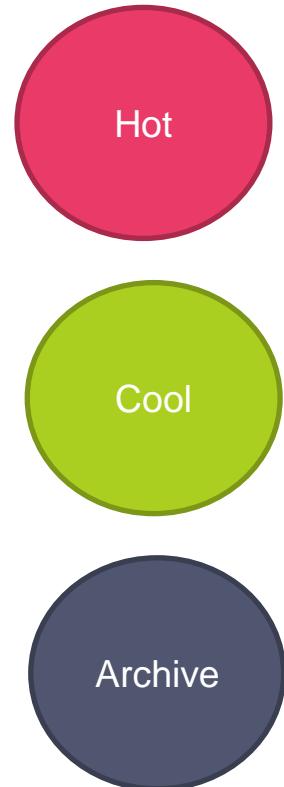


Storage Access Tiers

Organize your data based on attributes like frequency of access and planned retention period.

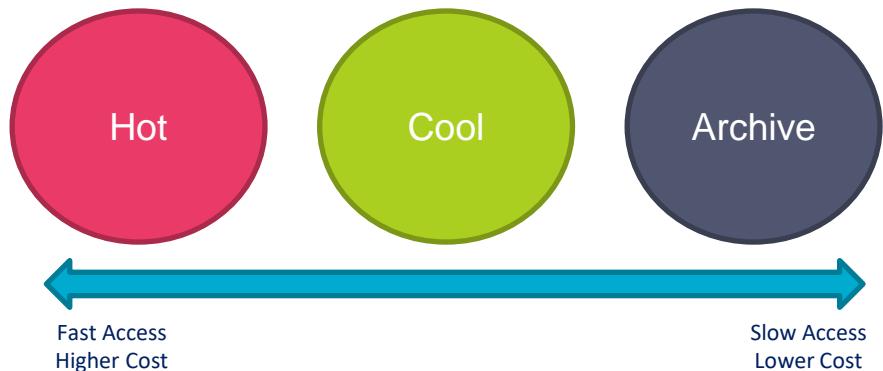
Storage Access Tiers

- Data stored in the cloud can be different based on how it's generated, processed, and accessed over its lifetime.
- Pricing
 - The volume of data stored/month
 - Types of operations performed
 - Number of operations performed
 - Data transfer cost, if any
 - The selected data redundancy option
- Organize your data based on attributes like frequency of access and planned retention period.
- Blob access tiers
 - Hot access tier
 - Cool access tier
 - Archive access tier



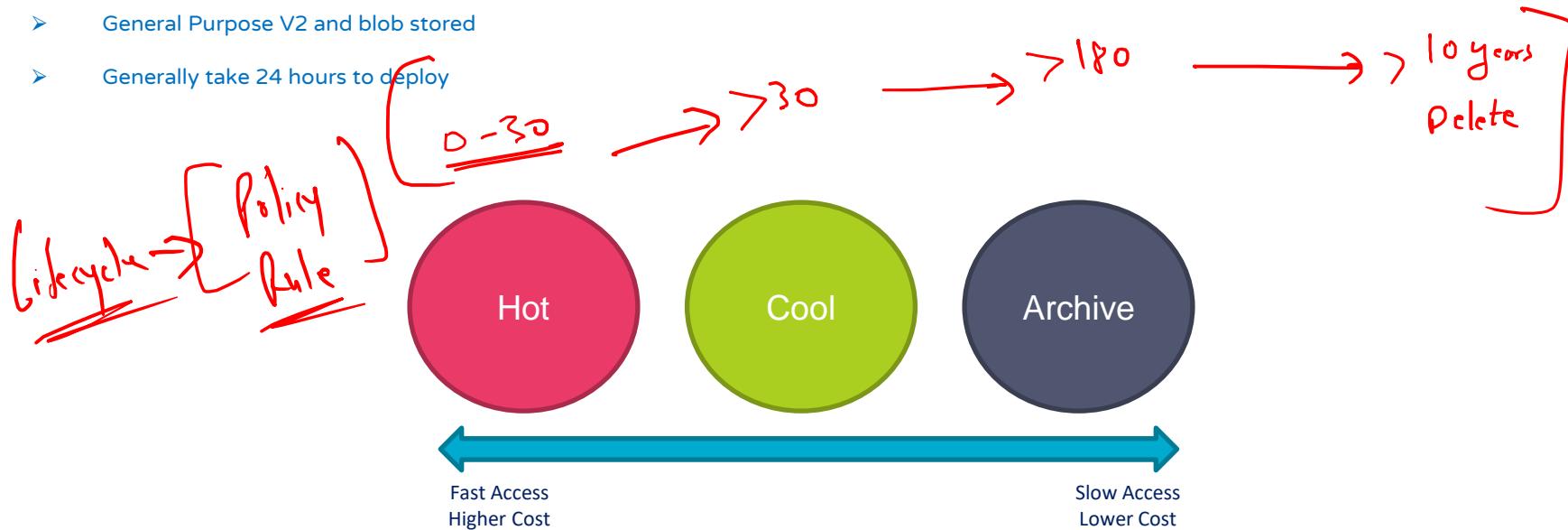
Storage Access Tiers

- **Hot**
 - Frequently accessed data
 - Example - images for your website
 - Low latency
 - Higher access cost
- **Cool**
 - Infrequent accessed data
 - Example - invoices for your customers
 - High latency
 - Lower cost
 - Stored for at least 30 days
- **Archive**
 - Rarely accessed data
 - Example - long-term backups
 - Highest access times and access cost
 - Latency in hours
 - Stored for at least 180 days
 - Use Case: Business policy mandated Data Archiving, long term retention like healthcare data



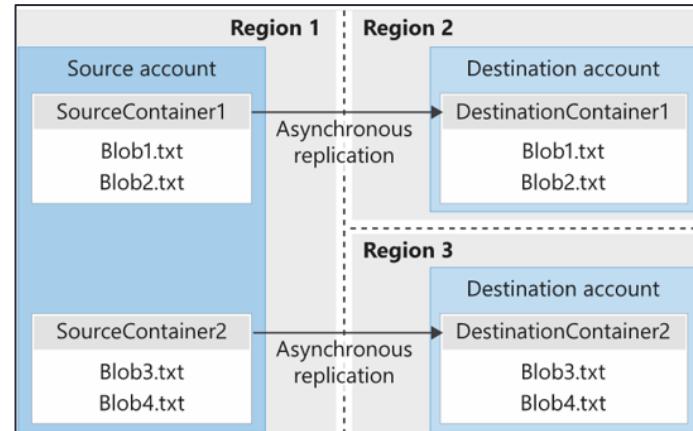
Blob lifecycle management

- Transition blobs to a cooler storage tier (hot to cool, hot to archive, or cool to archive) to optimize for performance and cost.
- General Purpose V2 and blob stored
- Generally take 24 hours to deploy



Blob object replication

- Copy data from source to destination storage account
- A replication policy includes one or more rules that specify a source container and a destination container and indicate which block blobs in the source container will be replicated.
- What exactly copy?
 - All versions Blob
 - Blob's metadata
 - Blob's properties
 - NOT – snapshots are not copied
- Both the source and destination accounts should have:
 - Versioning enable
 - Either from Hot and Cool tier
- Scenarios
 - Minimize read request latency
 - Process data at single location and replicate results across multiple regions so that users in regions only access the results instead of entire dataset.
- Consider Cost while replicating



Blob object replication



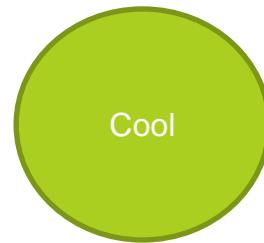
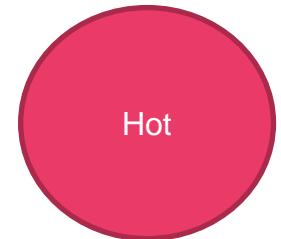
- Source Storage
- Location – East US
- Enable Versioning and change feed
- Create Replication Rules at source
- Destination Storage
- Location - India
- Enable Versioning

Azure File Share Performance Tier

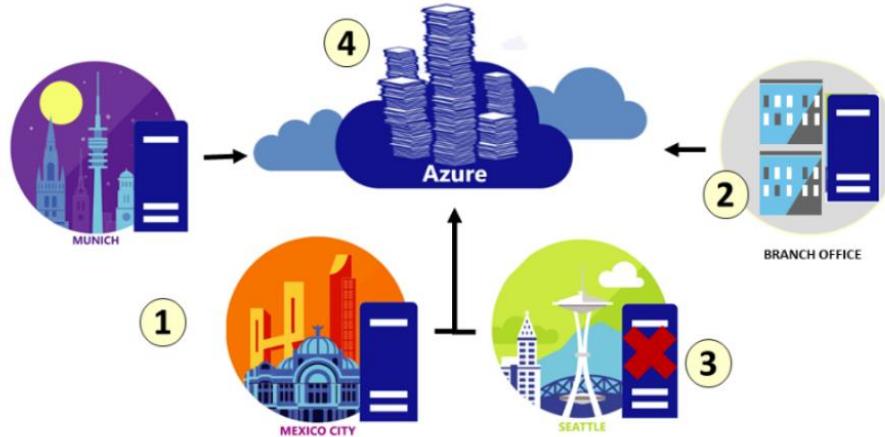
	Performance Tier	Max Size	Access Tiers	Replication Options
General Purpose V2	Standard	5 TB default (up to 100 TB on request)	Hot, Cool, Transaction Optimized	LRS, GRS, ZRS, GZRS
File Storage	Premium	100 TB default	N/A	LRS, ZRS

Azure File Access Tier

- Different Access tiers have different costs for storage and access to data.
- Hot
 - Optimized for general purpose file sharing scenarios
 - Organization file shares and using with Azure File Sync.
 - Storage cost – Higher
 - Cost to access - Lower
- Cool
 - Cost-efficient storage
 - Optimized for online archive storage scenarios.
 - Storage Cost – Lower
 - Cost to access – Higher
- Transaction optimized
 - For transaction-heavy workloads that don't need the lower latency that might be offered with premium file shares, but has consistency.
 - Highest cost from a storage standpoint.
 - Lowest cost per transaction compared to the hot and cool tier.
 - Great fit for applications that require file storage or for back-end storage for your applications.
- Access tier can be change for specific file shares as needed

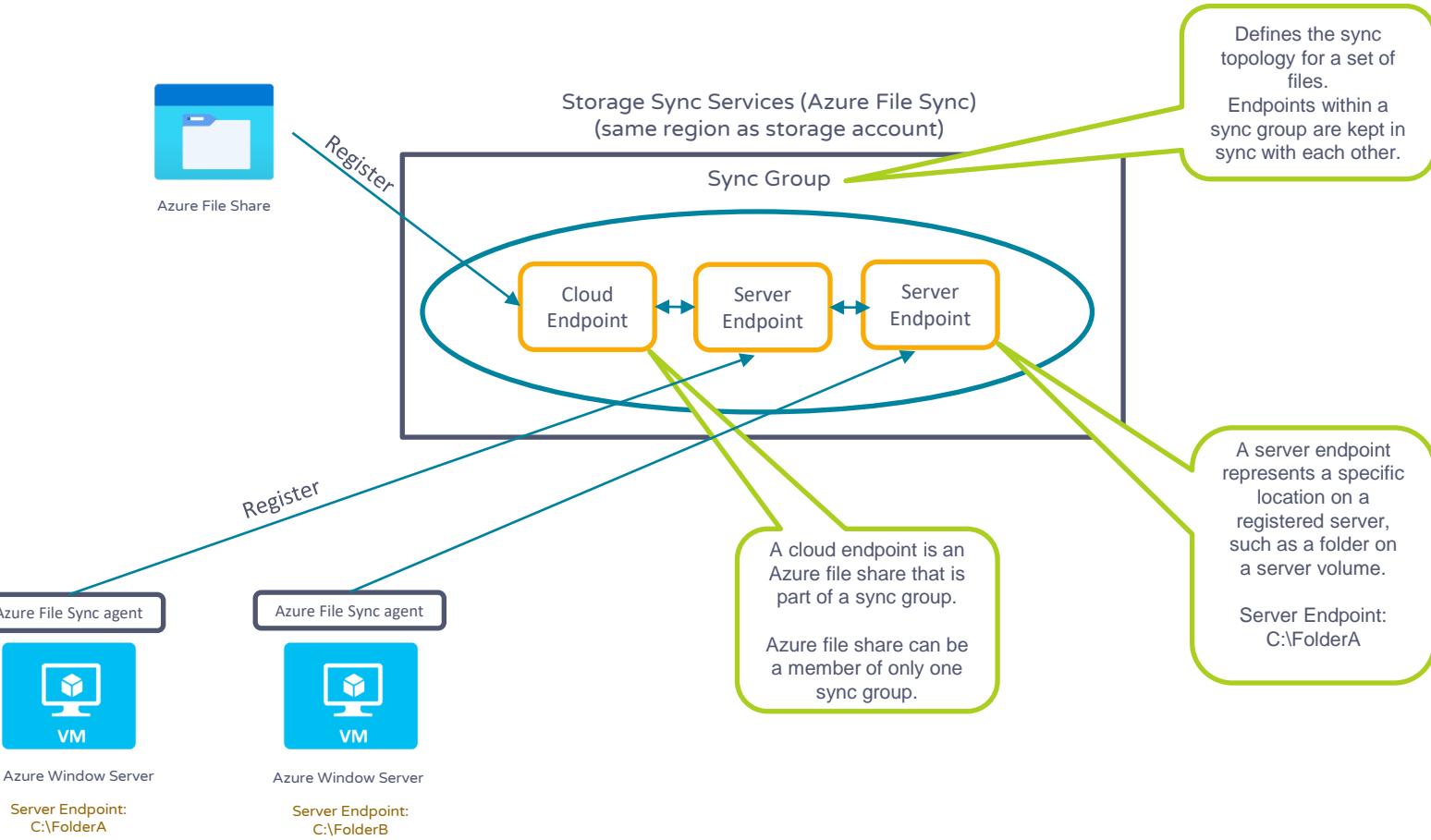


Azure File Sync

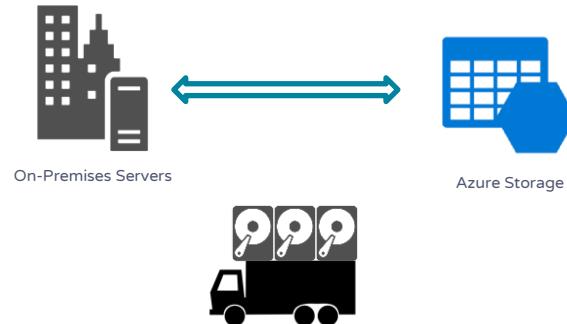


- Replication occurs between Windows servers in your data centers and Azure.
- Provide local caching for your users. You can have as many caches as you want.
- By default, all files are tied to Azure Files, but with Cloud Tiering enabled, only frequently accessed files are cached locally on the server.
- You can access your data locally using SMB, NFS, or FTPS on Windows Server.
- Advantages
 - Lift and shift
 - Backup and Disaster Recovery
 - File Archiving

Azure File Sync Implementation

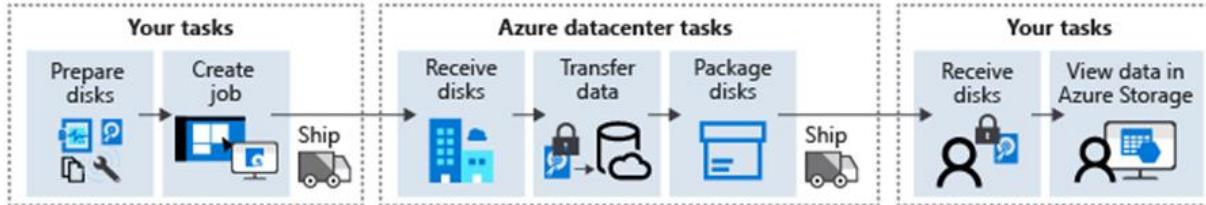


Import and export service

- Move small amount of data – Internet
 - AzCopy
 - Azure Storage Explorer
 - Move large amount of data (TBs) between on-premises and Azure storage securely.
 - Scenarios
 - Migrating data to the cloud
 - Backup
 - Data recovery
 - Issues
 - Network is slow
 - Getting more network bandwidth is cost-prohibitive
 - Solution
 - Ship disk drive physically
 - Disk drive – you can use your own or ones provided by Microsoft.
 - Own - Solid-state drives (SSDs) or Hard disk drives (HDDs)
 - Microsoft – Azure Data Box
 - Import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.
 - Export large amounts of data from Azure Blob storage to disk drives and ship to your on-premises sites.
- 

Import jobs

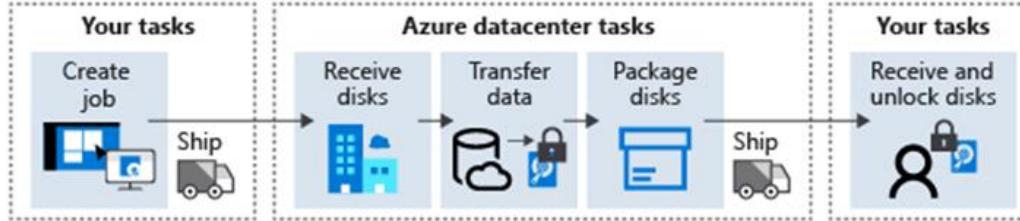
Import data with Azure Import/Export



- Note: Import large amounts of data to Azure Blob storage and Azure Files
- Prepare disks
 - Use [WAImpoerExport](#) tool to copy the data to disk/drive
 - Generate journal files
 - Journal file stores basic information such as drive serial number, encryption key, and storage account details.
 - Use [BitLocker](#) to encrypt the drive
- Create import job
 - Refer Azure Storage Account
 - Specify the shipping and receiving address
- Ship the disks to the destination that you specified when creating the import job
- Update the job by providing the shipment tracking number.

Export jobs

Export data with Azure Import/Export



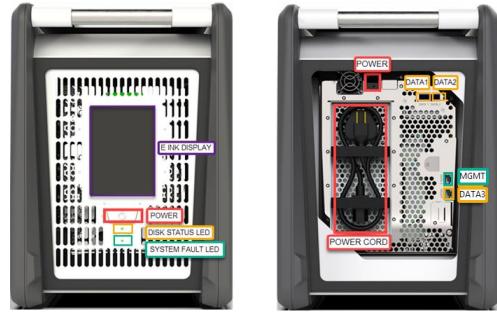
- Export large amounts of data from Azure Blob storage
- Identify the data and number of disks using WAImpoErtExport tool
- Create Export Job
 - Specify Azure Storage account -> Blobs
 - Return address
- Ship the disk
 - Ship the disk to the Azure region hosting the storage account
 - Update the job by providing the shipment tracking number
- Azure datacenter tasks
 - Receive and copy the data
 - Encrypt the data using Bitlocker
 - Ship them back
- Your tasks
 - Bitlocker keys will be available on Azure portal.
 - Unlock and verify drive with WAImpoErtExport unlock command
 - Copy data to your on-premises storage

Import/Export Tool (WAImpExp)

- Command line tool, downloadable from Microsoft
- Need 64-bit windows only, no Linux or MacOS support
- What it does?
 - Determine number of drives needed for export job
 - Data copy
 - Encryption or decryption of drive with BitLocker
 - Creation of journal files needed for import jobs
- Two versions
 - Version 1 is for import/export for Azure Blob storage
 - Version 2 is for import of Azure Files
- The Azure Import/Export Tool prepares and repairs drives for the Microsoft Azure Import/Export service.
 - Before Import job – copy data to hard drives
 - After import job - repair any blobs that were corrupted, were missing, or conflicted with other blobs.
 - Before an export job – Identify the number of drives needed for export jobs.
 - After an export job - you can use this tool to repair any corrupted or missing files on the drives.

Azure Data Box

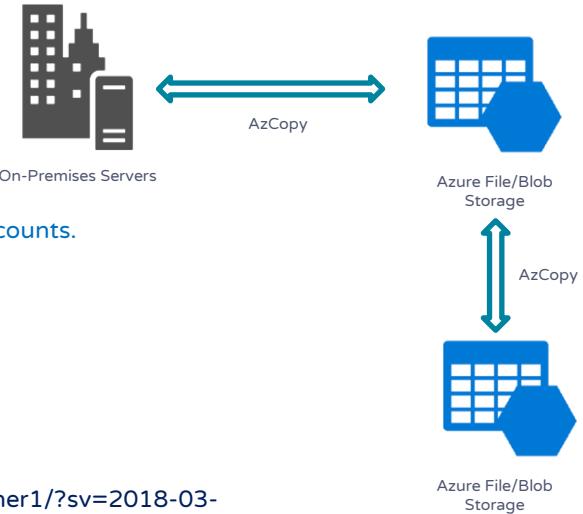
- Microsoft provides you a piece of hardware **in three different sizes** developed specifically for import and export tasks.
- You can order the Data Box device via the Azure portal to import or export data from Azure.
- Ideally suited to transfer data sizes larger than 40 TBs
- Scenarios: Onetime migration, Initial bulk transfer, Disaster recovery, Migrate back to on-premises or to another cloud service provider



Data Box front view (left) and back view (right)

AzCopy

- Command-line utility
- Available to download and install on Windows, Linux, and Mac
- Use it to copy data to/from Microsoft Azure Blob and File storage
 - you can copy data between a file system and a storage account, or between storage accounts.
- AzCopy is preinstalled in Azure Cloud Shell, so you can use it there if you can't run it locally.
- Simple commands
 - List of available commands: `azcopy --help`
 - Basic syntax for AzCopy commands: `azcopy copy [source] [destination] [flags]`
 - `azcopy copy "C:\local\path" "https://account.blob.core.windows.net/mycontainer1/?sv=2018-03-28&ss=bjqt&srt=sco&sp=rwddgcup&se=2019-05-01T05:01:17Z&st=2019-04-30T21:01:17Z&spr=https&sig=MGCXiEzbttkr3ewJlh2AR8KrghSy1DGM9ovN734bQF4%3D" --recursive=true`
- Authentication options



Storage type	Currently supported method of authorization
Blob storage	Azure AD & SAS
Blob storage (hierarchical namespace)	Azure AD & SAS
File storage	SAS only

Move VMs

- You can move VMs and related resources to different resource group or subscriptions.
- Why you need to move?
 - If you created a VM in a personal subscription and want to move it to your company's subscription to continue working.
- Do not need to stop the VM in order to move it and it should continue to run during the move.
- The move creates new resource IDs. After moving the VM, update your tools and scripts to use the new resource IDs.
- When switching subscriptions, all v-net resources must be moved.
- It is not possible to move VM scale sets with standard load balancers and standard Public IP.
- Virtual machines that use a key vault for disk encryption can't be moved.
 - You can disable the encryption and then move
- Prior to moving, restore points on VMs configured with Azure backup must be deleted.



Redeploy Virtual Machines

- Redeploying a Azure virtual machine (VM) may help troubleshoot Remote Desktop (RDP) or application access issues.
 - Cannot connect via RDP or SSH
 - If you are not able to access applications on VMs
- Steps: Power off VM, move to a new node, and then power back on
- Retain all configuration options and resources.
- All data saved on the temporary disks will be lost.
- The virtual network interface's dynamic IP addresses will be updated.
- Use Azure PowerShell or Azure portal.



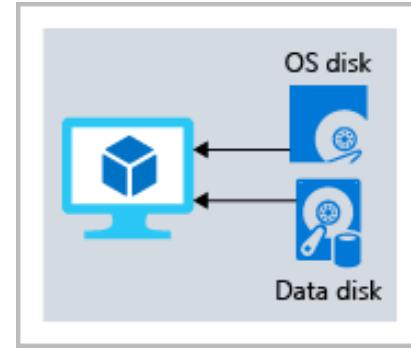
Disk Storage



High-performance, highly durable block storage for Azure Virtual Machines

Disk Storage

- VM uses disks as a place to store an operating system, applications, and data in Azure.
 - These are like physical disk in an on-premises server but, virtualized.
- Types of Disks
 - **Standard hard disk drives (HDD)** - Backup, non-critical, infrequent access
 - **Standard solid-state drives (SSD)** - Web servers, lightly used enterprise applications and dev/test
 - **Premium solid-state drives (SSD)** - Production and performance sensitive workloads
 - **Ultra disks** - IO-intensive and other transaction-heavy workloads.
- One virtual machine can have one OS disk and multiple Data disk
- One data disk can only be link with one VM
- Both the OS disk and the data disk are virtual hard disks (VHDs) stored in an Azure storage account.



Disk Storage

➤ Benefits

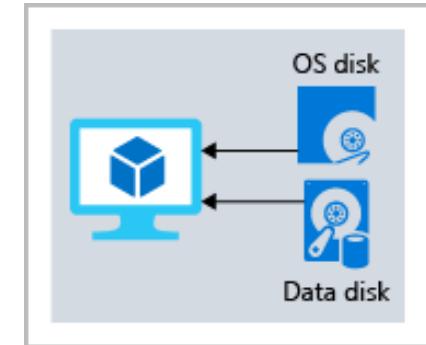
- Highly available (three replicas) – 99.999% availability
- Scalable – 50,000 VM disks
- Granular access control - Use RBAC to assign specific permissions for a managed disk to one or more users.
- Integration with availability sets and Availability Zones, Backups and so on

➤ Security

- Private links – allow you to generate SAS token
- Encryption
 - Server-side encryption – data encryption-at-rest, default
 - Azure Disk encryption - encrypt the OS and Data disks

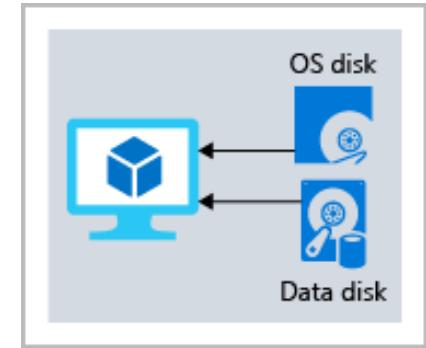
➤ Disk Roles

- OS Disk – Pre-installed OS, contain boot volume
- Data Disk – Store application data
- Temporary Disk
 - Short-term storage for applications and processes
 - May be lost during a maintenance or redeploy.
 - Successful reboot will persist data.



Latency vs IOPS vs Throughput

- **Latency** is a time taken to respond to an I/O request
- **IOPS** is a unit of measurement for the number of read and write operations performed per second.
 - Number of read write operations mostly useful for OLTP transactions used in Azure for DBs like SQL Server.
 - Latency is proportional to IOPS
- **Throughput** refers to the quantity of data read or written per second.
 - Measured in MB per second
 - Mainly a unit for high data transfer applications like big data Hadoop, Kafka streaming



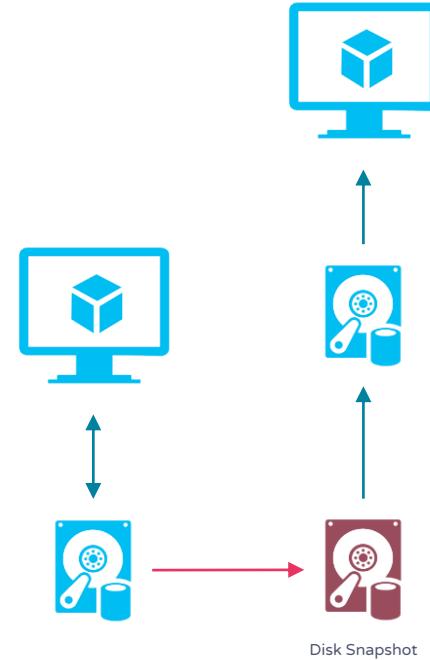
Disk Types

	Ultra disk	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA , top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 gibibyte (GiB)	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	4,000 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	160,000	20,000	6,000	2,000

- You can change an ultra disk's performance parameters without having to restart your virtual machines.
- Ultra disks can't be used as OS disks, they can only be created as empty data disks. Ultra disks also can't be used with some features and functionality, including disk snapshots, disk export, changing disk type, VM images, availability sets, Azure Dedicated Hosts, or Azure disk encryption.

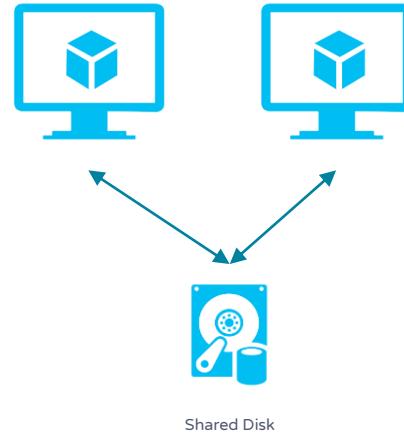
Snapshot

- A snapshot is a full, read-only copy of a virtual hard disk (VHD).
- You can take a snapshot of both operating system (OS) or data disk VHDs.
- Use Case:
 - Point-in-time backup
 - Restore or rebuild a VM
 - Troubleshoot virtual machine (VM) issues



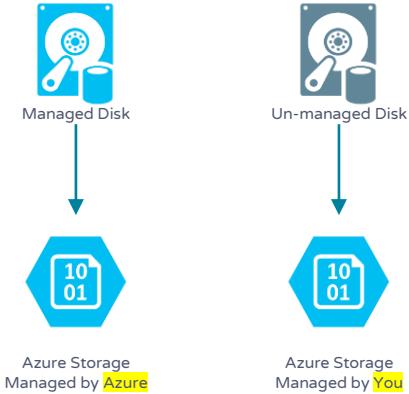
Azure Shared Disks

- Allow you to attach a managed disk to multiple virtual machines (VMs) simultaneously.
- Only ultra disks, premium SSDs, and standard SSDs can enable shared disks
- Shared managed disks do not come with a fully managed file system accessible through SMB/NFS.
- Use a cluster manager like Windows Server Failover Cluster (WSFC) or Pacemaker to handle cluster node communication and write locking.



Managed vs Unmanaged Disk

- Managed Disks
 - Managed by Azure
 - High availability, secure
 - Azure create storage account behind the scene
- Un-managed Disks
 - Not Managed by Azure
 - You create storage account
 - Full control over data
 - You have to take care of encryption, data recovery plans etc.
- You cannot create both managed and unmanaged disks on a VM



Virtual Machine Networking

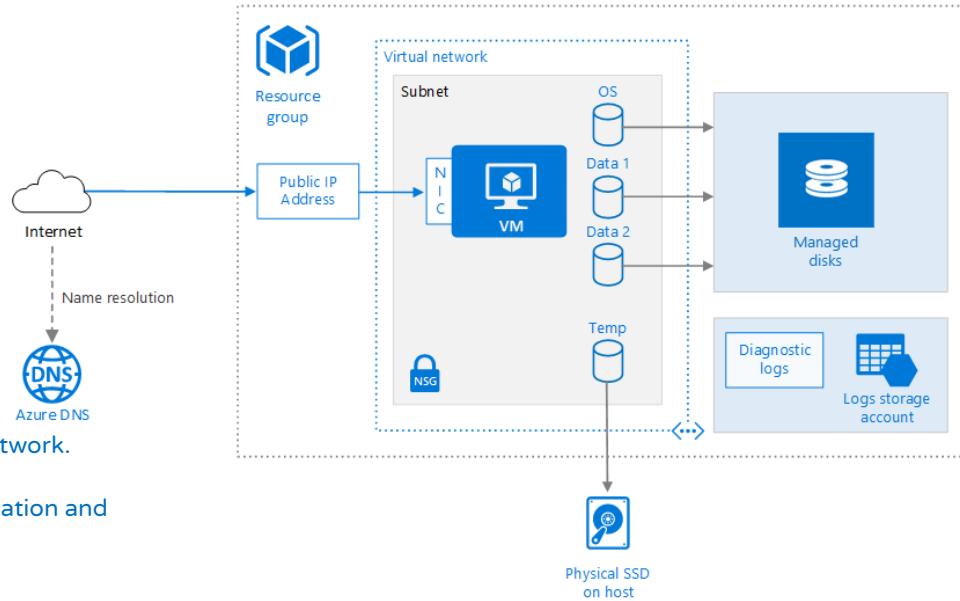
- Virtual Network (VNet) enables Azure resources to securely communicate with each other

- Subnets:

- Divide a network into two or more networks
- A subnet is a range of IP addresses in the virtual network.
- For organization and security.
- No security boundary b/w subnets by default

- Network Interface Card (NIC)

- Interconnection between a virtual machine and a virtual network.
- **IMP:** Each NIC attached to a VM must exist in the same location and subscription as the VM.



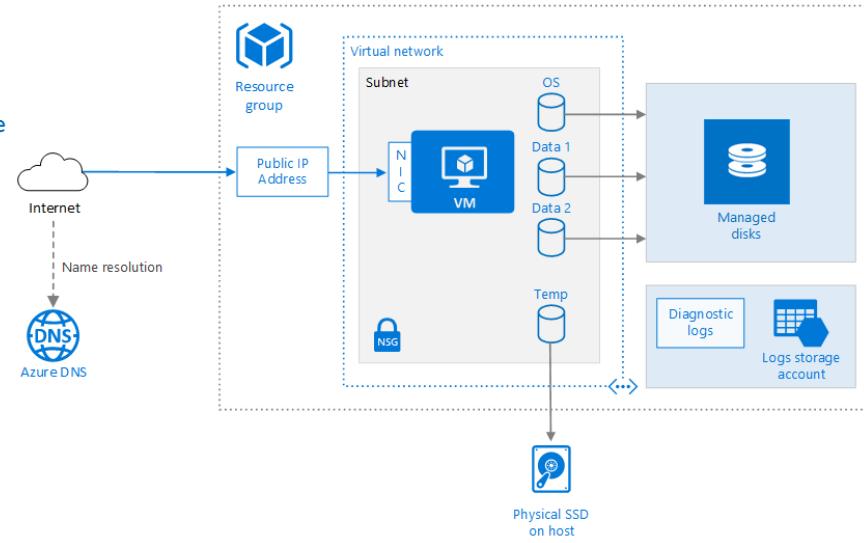
Virtual Machine Networking

➤ Network security group (NSG)

- Allow or deny network traffic to subnets, NICs, or both.
- NSGs can be associated with either subnets or individual NICs connected to a subnet.
- When an NSG is associated with a subnet, the ACL rules apply to all the VMs in that subnet. Traffic to an individual NIC can be restricted by associating an NSG directly to a NIC.

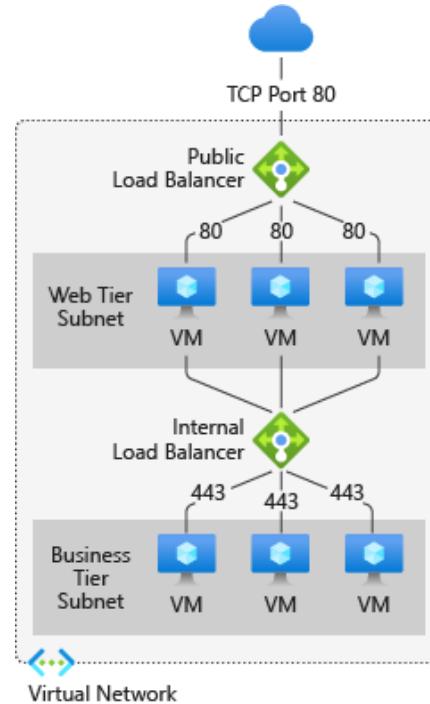
➤ IP addresses

- Enable Azure resources to communicate to Internet and public-facing Azure services.
- Can be dynamic (Default) or static.
- Reserve a static IP address if you need a fixed IP address that won't change — for example, if you need to add the IP address to a safe list.
- **IMP:** Deallocating your virtual machine releases your dynamic public IP

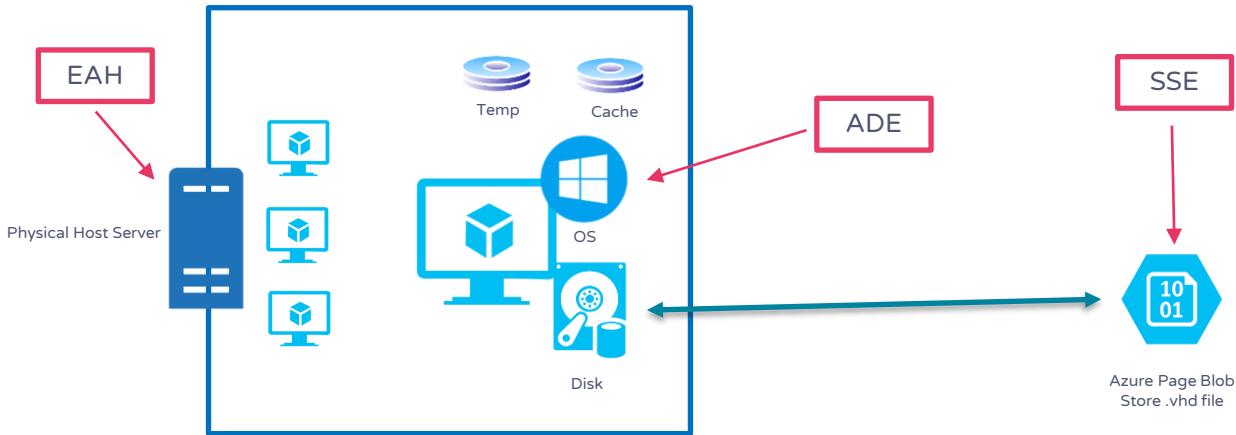


Virtual Machine Networking

- A load balancer balance or distribute incoming Internet traffic to multiple VMs
 - Public Load Balancers are used to load balance internet traffic to your VMs.
 - Internal load balancers are used to load balance traffic inside a virtual network.
- Azure Bastion
 - Provide secure management connectivity to virtual machines in a virtual network.
 - Enables connections without exposing a public IP on the VM.



Types of Disk Encryption

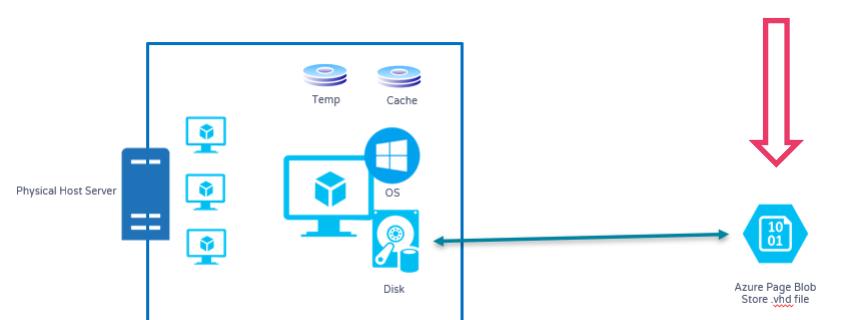


- **Server-Side Encryption** - encrypts your disks at the storage account level, at rest.
 - Default, always enabled, can't turn off.
- **Azure Disk Encryption** - encrypts your disks at the VM OS level.
 - Use BitLocker for Windows VMs and DM-Crypt for Linux VMs.
 - Data encrypt during transit
- **Encryption at host** – Also encrypt your temporary disk and cache at host.
 - Does not use your VM's CPU and doesn't impact your VM's performance.
 - Truly end-to-end encryption

Server-Side Encryption (SSE)

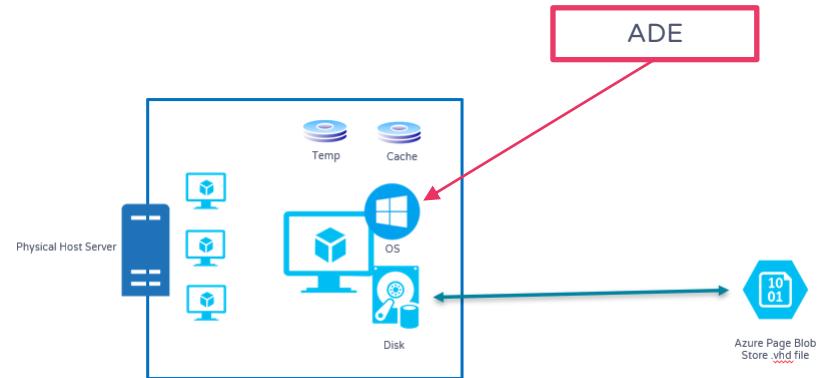


- Data at rest encryption.
- Protect the data on OS and data disks. Temporary disks are not encrypted.
- Does not impact the performance of managed disks.
- Use 256-bit AES encryption, one of the strongest block ciphers available, and 140-2 compliant.
- Encryption keys are managed through:
 - Platform Managed Keys (PMK) – Default, Microsoft manages (key is rotated, and backup)
 - Customer Managed Keys (CMK) – Customer manages, and is responsible for key store in Azure Key Vault or customer controlled hardware.



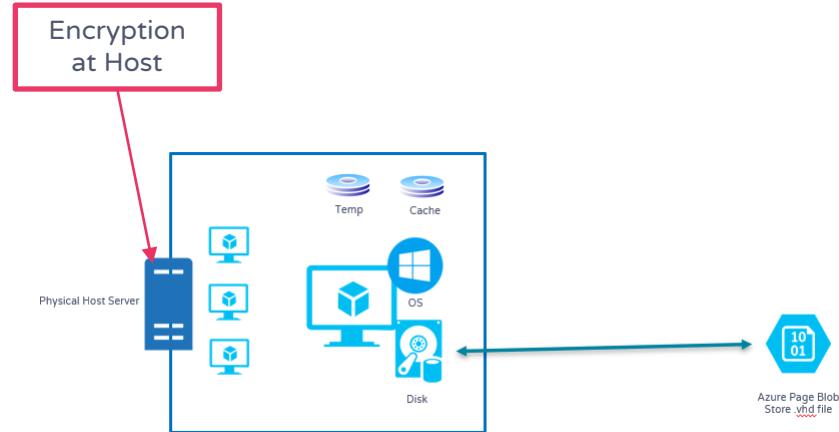
Azure Disk Encryption (ADE)

- Encrypted the disk at the operating system level.
- leverage Windows or Linux native encryption capabilities
 - Windows with BitLocker
 - Linux with DM-Crypt
- Temporary disk and OS/data disk caches are also encrypted
- Requires an Azure Key Vault to control and manage disk encryption keys and secrets
- Key vault and VMs must reside in the same Location and subscription
- ADE can only be paired with SSE with PMK



Encryption at host

- End-to-end encryption between the disk at rest and when the disk is allocated to and ran on a host.
- Eliminate the need for Azure Disk Encryption (ADE)
- Encryption at host does not use your VM's CPU and doesn't impact your VM's performance.
- Whatever is used to encrypt the disk encryption set at rest (PMK or CMK) will be used to encrypt the in transit data from the disk to the host. Also same PMK or CMK used to encrypt the cache disk.
- The temp disk will always be encrypted by a PMK
- Prerequisite: must enable the feature for your subscription



Server-Side Encryption

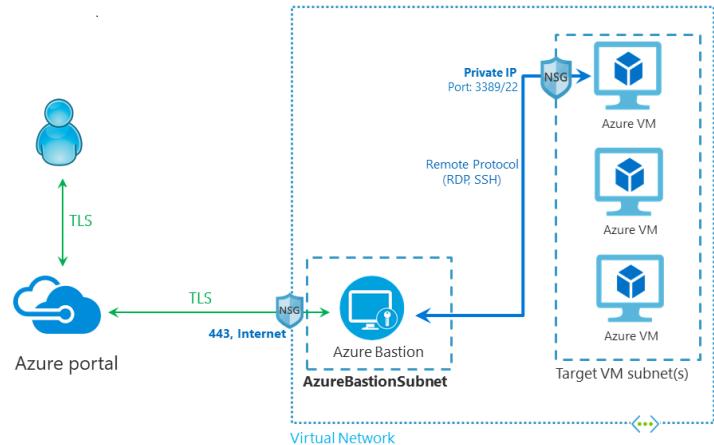
	Encryption at rest (OS and data disks)	Temp disk encryption	Encryption of caches	Data flows encrypted between Compute and Storage	Customer control of keys	Does not use your VM's CPU	Works for custom images
Encryption at rest with platform-managed key (SSE+PMK)	✓	✗	✗	✗	✗	✓	✓
Encryption at rest with customer-managed key (SSE+CMK)	✓	✗	✗	✗	✓	✓	✓
Azure Disk Encryption	✓	✓	✓	✓	✓	✗	✗ Does not work for custom Linux images
Encryption at Host	✓	✓	✓	✓	✓	✓	✓

Connect to Linux VM using SSH

- SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections.
- SSH is the default connection protocol for Linux VMs hosted in Azure.
- SSH Keys - Secure and preferred method of connecting to a VM using SSH is by using a public-private key pair
 - Public key is placed on your Linux VM, or any other service that you wish to use with public-key cryptography.
 - Private key remains on your local system. Protect this private key. Do not share it.
- As soon as you connect with an SSH client to your Linux VM, it verifies that you have the private key on your PC. The client gets access to the VM if it has the private key.

Azure Bastion

- Protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.
- No Public IP address required on the Azure VM
- Fully managed platform PaaS service from Azure

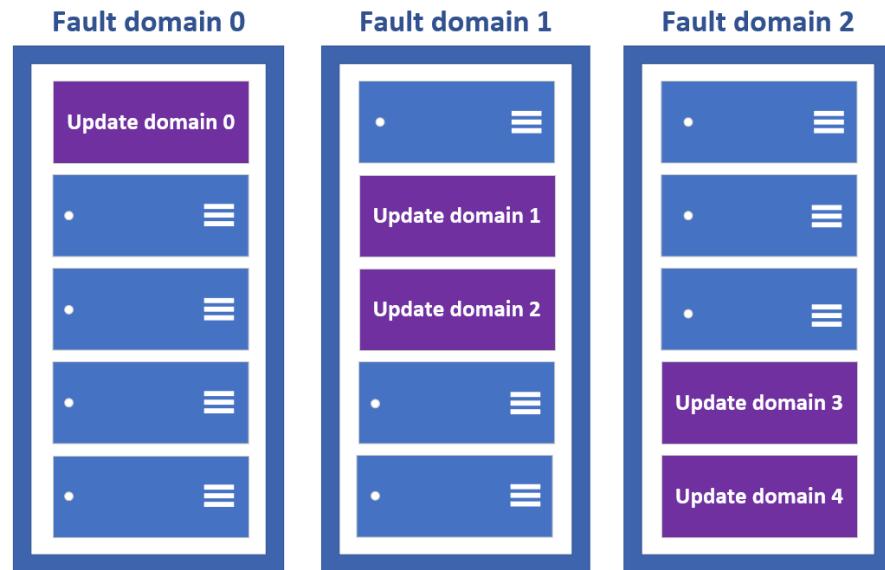


Availability sets

Provides High availability and Business continuity for applications

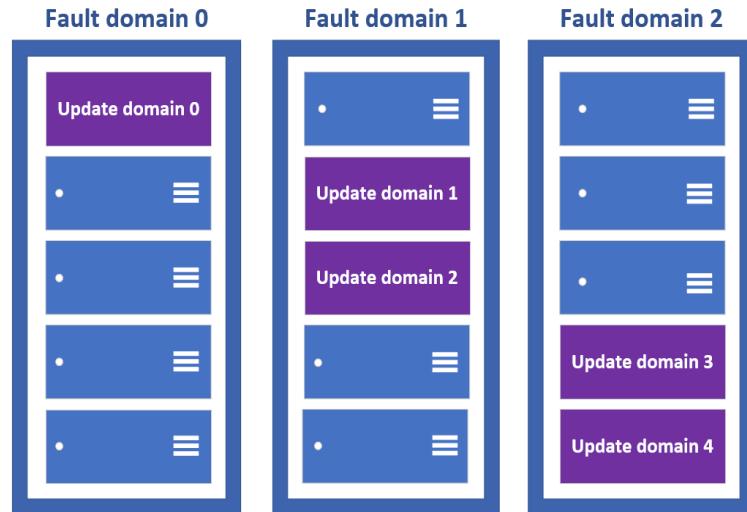
Availability Sets

- Availability Sets make use of two key concepts - Fault Domains, and Update Domains.
- **Update domains** define the group of virtual machines that are going to be patched/maintained/rebooted at same time.
- **Fault domains** define the group of virtual machines that share a common power source and network switch.
- It saves from rackwide failure, or a rackwide maintenance window that can take down all VMs hosted on this single point of failure.
- Availability sets are free to use! You only pay for the virtual machines being created.
- It does not protect your application from operating system or application-specific failures, it does limit the impact of potential physical hardware failures, network outages, or power interruptions.



Availability Sets - SLA

- Prevent a single point of failure and from being upgraded at the same time
- VMs placed in an availability set should perform an identical set of functionalities and have the same software installed.
- For all Virtual Machines that have two or more instances deployed in the same Availability Set, we guarantee you will have Virtual Machine Connectivity to at least one instance at least **99.95%** of the time.
- VM can only be added to an Availability Set when it is created.
 - Else, delete and recreate VM

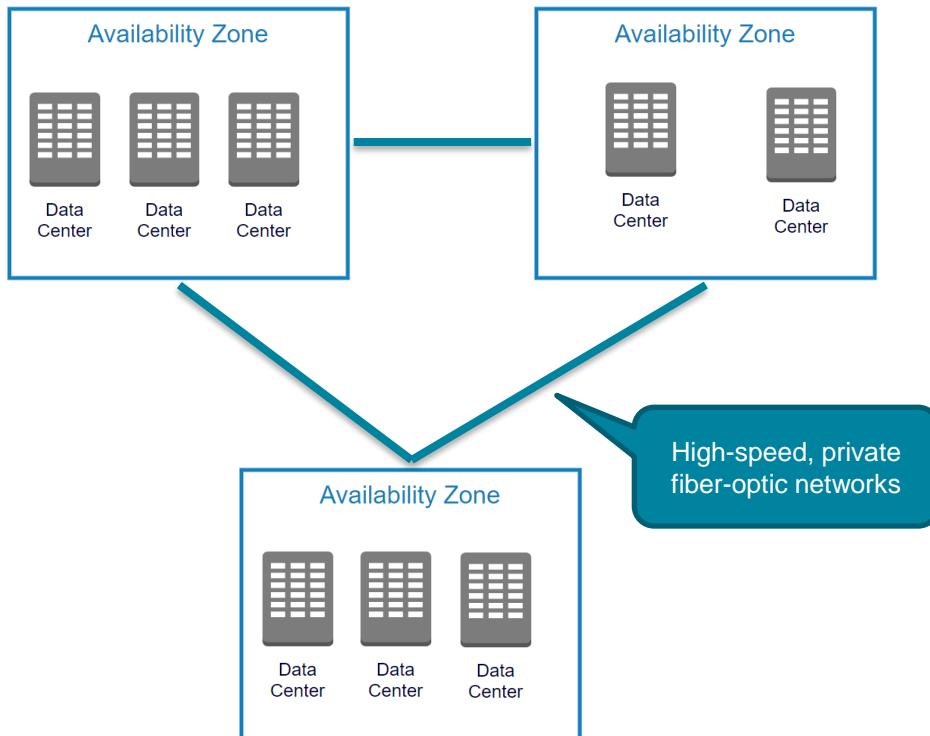


Availability Zones

High availability for your mission-critical applications and data

Availability Zones

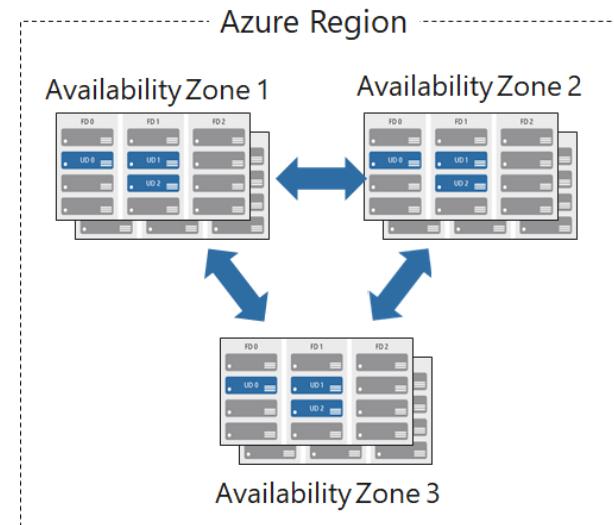
F Region



- Each Availability Zone has a distinct power source, network, and cooling.
- If one zone is compromised, then replicated apps and data are instantly available in another zone.
- It's your responsibility to sync applications between different VMs.

VM in Availability Zones - SLA

"For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time."

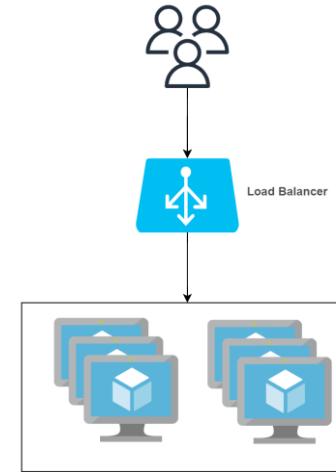


Virtual Machines Scale Sets

Manage and scale up to thousands of Linux and Windows VMs

Virtual Machines Scale Sets

- Create and manage a group of load balanced VMs.
- Allows your application to automatically scale as resource demand changes
 - The number of VM instances can automatically increase or decrease in response to demand or a defined schedule.
- All VM instances are created from the same base OS image and configuration.
 - VM size, disk configuration, and application installs should match across all VMs.
- Provides high availability and application resiliency
 - Can use availability zones or availability sets
- There is no cost for the scale set itself, you only pay for each VM instance that you create.

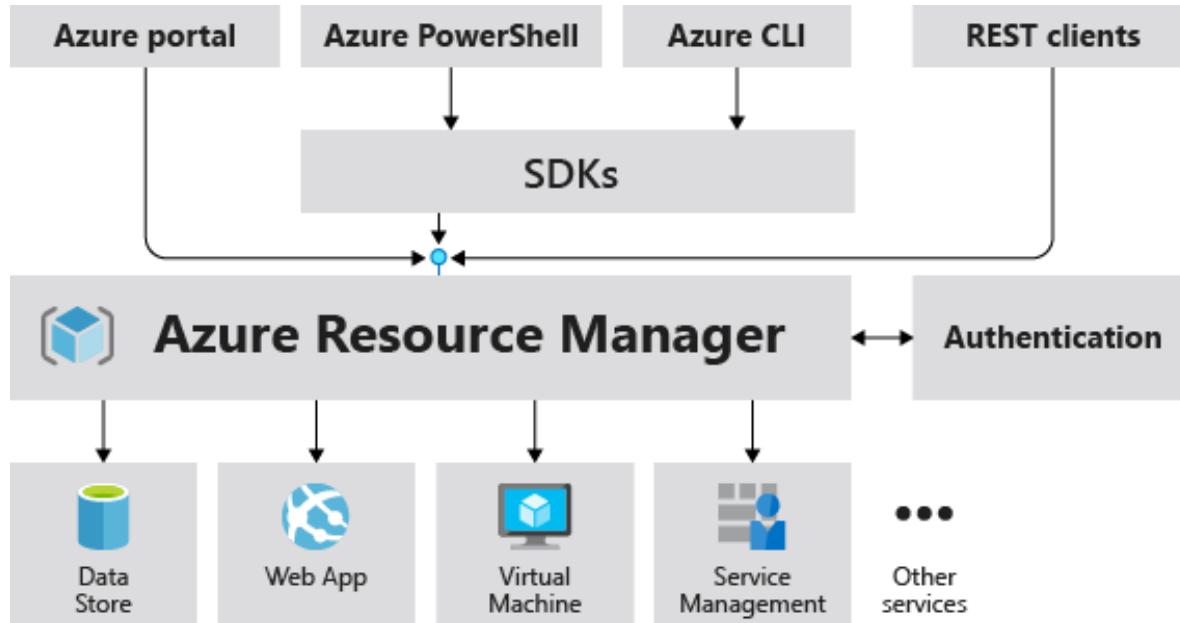


Scenario	Manual group of VMs	Virtual machine scale set
Add extra VM instances	Manual process to create, configure, and ensure compliance	Automatically create from central configuration
Traffic balancing and distribution	Manual process to create and configure Azure load balancer or Application Gateway	Can automatically create and integrate with Azure load balancer or Application Gateway
High availability and redundancy	Manually create Availability Set or distribute and track VMs across Availability Zones	Automatic distribution of VM instances across Availability Zones or Availability Sets
Scaling of VMs	Manual monitoring and Azure Automation	Autoscale based on host metrics, in-guest metrics, Application Insights, or schedule

Azure Resource Manager (ARM)

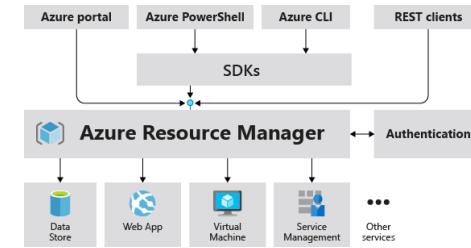
Deployment and management service for Azure

Azure Resource Manager



Azure Resource Manager

- Deployment and management service for Azure
- All Azure resource activities are routed via ARM.
- Describe the resources in a declarative JSON format
- ARM template is verified before any code is executed to ensure that the resources will be created and connected correctly
- Automatic Rollback in case of failure
- The template then orchestrates the creation of those resources in parallel
- Templates can even execute PowerShell and Bash scripts before or after the resource has been set up
- Creates all dependencies in the correct order
- Save previous scripts for version control
- ARM templates define your application's infrastructure requirements for a repeatable deployment that is done in a consistent manner
- Why not PowerShell or CLI?
 - No validation step in these tools
 - If a script encounters an error, the dependency resources can't be rolled back easily
 - Deployments happen serially
 - You have to figure out dependencies



ARM Template Structure



- **Schema:** defines the location of the JSON file that describes the version of the template language.
- **Content version:** Version of the template. Use this value to document significant changes in your template.
- **apiprofile:** an API version that serves as a collection of API versions for resource types.
- **Parameters:** Values that are provided when deployment is executed to customize resource deployment.
- **Variables:** Values used in templates as JSON fragments to simplify template language expressions.
- **Functions:** User-defined functions that are available within the template.
- **Resources:** Resource types that are deployed or updated in a resource group or subscription.
- **Outputs:** Values that are returned after deployment.

Virtual machines extensions

- Automate the repetitive work of post-deployment configuration and tasks on Azure VMs.
 - Software installation, anti-virus protection, or a configuration script inside
- 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.

Custom Script Extensions

- The Custom Script Extension downloads and runs scripts on Azure virtual machines (VMs).
- This extension is useful for post-deployment configuration, software installation, or any other configuration or management task.
 - Example: Install IIS on Windows server, or Apache on a Linux server with a web app
- You can download scripts from Azure Storage or GitHub, or provide them to the Azure portal at extension runtime.
- You can add extensions in the new or existing instance as well
- Can integrates with Azure Resource Manager templates.
- Script only runs once, schedule a task to run again
- Removing the extension does not undo what the script did
- You can also run it by using the Azure CLI, PowerShell, the Azure portal, or the Azure Virtual Machines REST API.
- **Considerations**
 - **Timeout.** Custom Script extensions have 90 minutes to run.
 - **Dependencies.** If your extension requires networking or storage access, make sure that content is available.
 - **Failure events.** Be sure to account for any errors that might occur when running your script.
 - For example, running out of disk space, or security and access restrictions. What will the script do if there is an error?
 - **Sensitive data.** Your extension may need sensitive information such as credentials, storage account names, and storage account access keys. How will you protect/encrypt this information?
 - **Reboot:** It's best to avoid including reboots in the script because the extension will stop working after the reboot. As a result, if you have any other commands that require the extension to run after the reboot, they will not run.
 - If you need rebook, look for other solutions like Desired state configuration, chef or puppet

VM Images

- Image: This is a copy of the full VM (include OS and data disks)
- After you build and customize a virtual machine, you can save the new image as a set of VHDs.
- You can put this new image in to Azure compute gallery.
- Two types of Images
 - Specialized VM images: copy of a live virtual machine
 - Copy of the configured operating system, software, user accounts, databases, connection information, and other data for your system.
 - Use as a backup of your system at a particular point in time, you can restore your virtual machine from this image a
 - New VM created out of image will have same host name, user accounts, and other settings
 - Generalized VM Images: No information retained.
 - Original VM is unusable after you perform the process
 - Tools for preparing a virtual machine for generalization –
 - For Windows, use the Microsoft System Preparation (Sysprep) tool.
 - For Linux, use the Windows Azure Linux Agent (waagent) tool.

Azure App Service

enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs

Azure App Service



- Enables you to host and manage your web applications
- Platform as a service (PaaS) environment
 - Focus on the business value and logic
 - Azure handles the infrastructure
 - Automatic scaling and high availability
- Programming language of your choice
- Supports Windows and Linux
- Automated deployments from GitHub or Azure DevOps
- Pay only for compute resources your app uses
 - App Service plan determines how much hardware is devoted to your application

Types of app services

- Web apps
 - Full support for hosting websites and web applications
 - Language: ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python.
 - Operating System: Windows or Linux
 - Web apps for containers can host your existing container images.
- API apps
 - Build REST-based web APIs
 - Choice of language and framework
 - Can be consumed from any HTTP- or HTTPS-based client.
- WebJobs
 - Run a program (.exe, Java, PHP, Python, or Node.js)
 - Run a script (.cmd, .bat, PowerShell, or Bash)
 - Can be scheduled or run by a trigger
 - Often used to run background tasks as part of your application logic.
- Mobile apps
 - Quickly build a back end for iOS and Android apps
 - Store mobile app data in a cloud-based SQL database.
 - Authenticate customers against common social providers, such as MSA, Google, Twitter, and Facebook.
 - Send push notifications.
 - Execute custom back-end logic in C# or Node.js.



App Service Backup

- App configuration, file content and database connected to your app
- Can backup manually or scheduled
- Can perform partial and full backups
- Backups are visible on the containers page of storage account
- Must have standard premium or isolated app service plan
- Must have an azure storage account and container in same subscription account
- Backups max out at 10GB of app and database content
- Backups of TLS enabled Azure Database for MySQL and PostgreSQL are not supported.



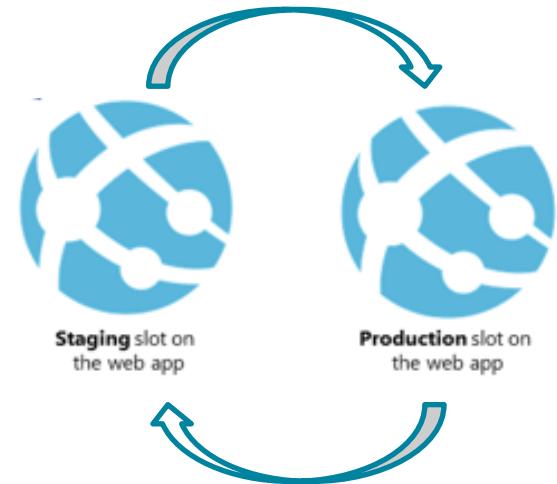
App Service Backup

- lets you easily create app backups manually or on a schedule.
- Can restore the app by overwriting the existing app or restoring to another app.
- Backup files store in storage account in same subscription.
- What gets backed up: App configuration, file content and database connected to your app
- Must have standard premium or isolated app service plan
- Backups can be up to 10 GB of app and database content.
- Backups of TLS enabled Azure Database for MySQL and PostgreSQL are not supported.
- Partial backups are supported. Partial backups allow you choose exactly which files you want to back up.
- Using a firewall enabled storage account as the destination for your backups is not supported.



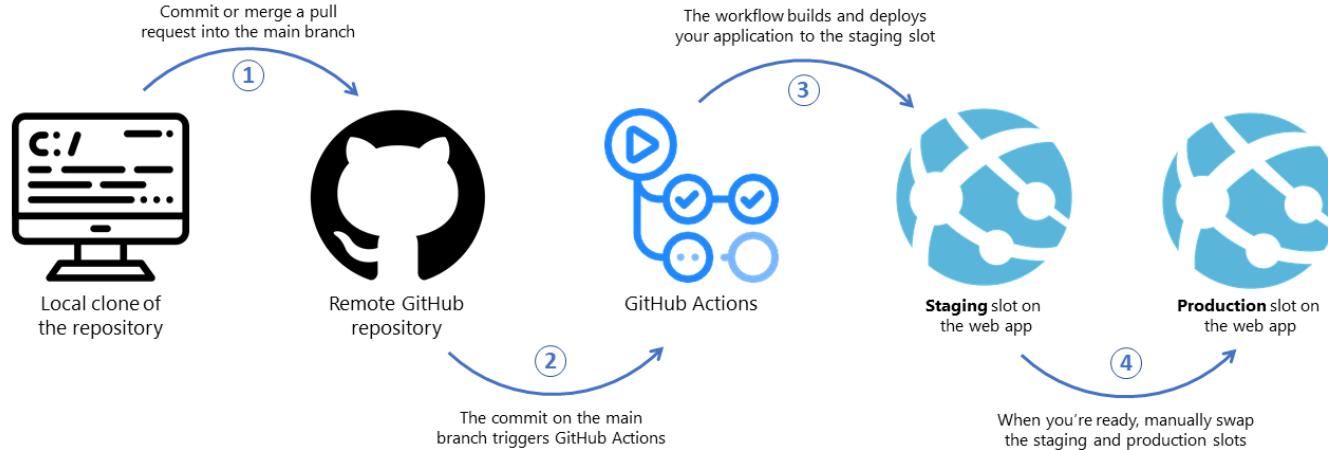
Deployment Settings

- You can test and validate changes in staging deployment slot before pushing them to production slot.
- After validation, you can simply swap staging and production slot.
- There is no downtime in this swap. No requests are lost due to traffic redirection.
- If rollback required, simply swap again.
- When pre-swap validation is not required, Auto Swap can be configured to automate the whole workflow.



Deployment Settings

A bird's-eye view of the CI/CD process

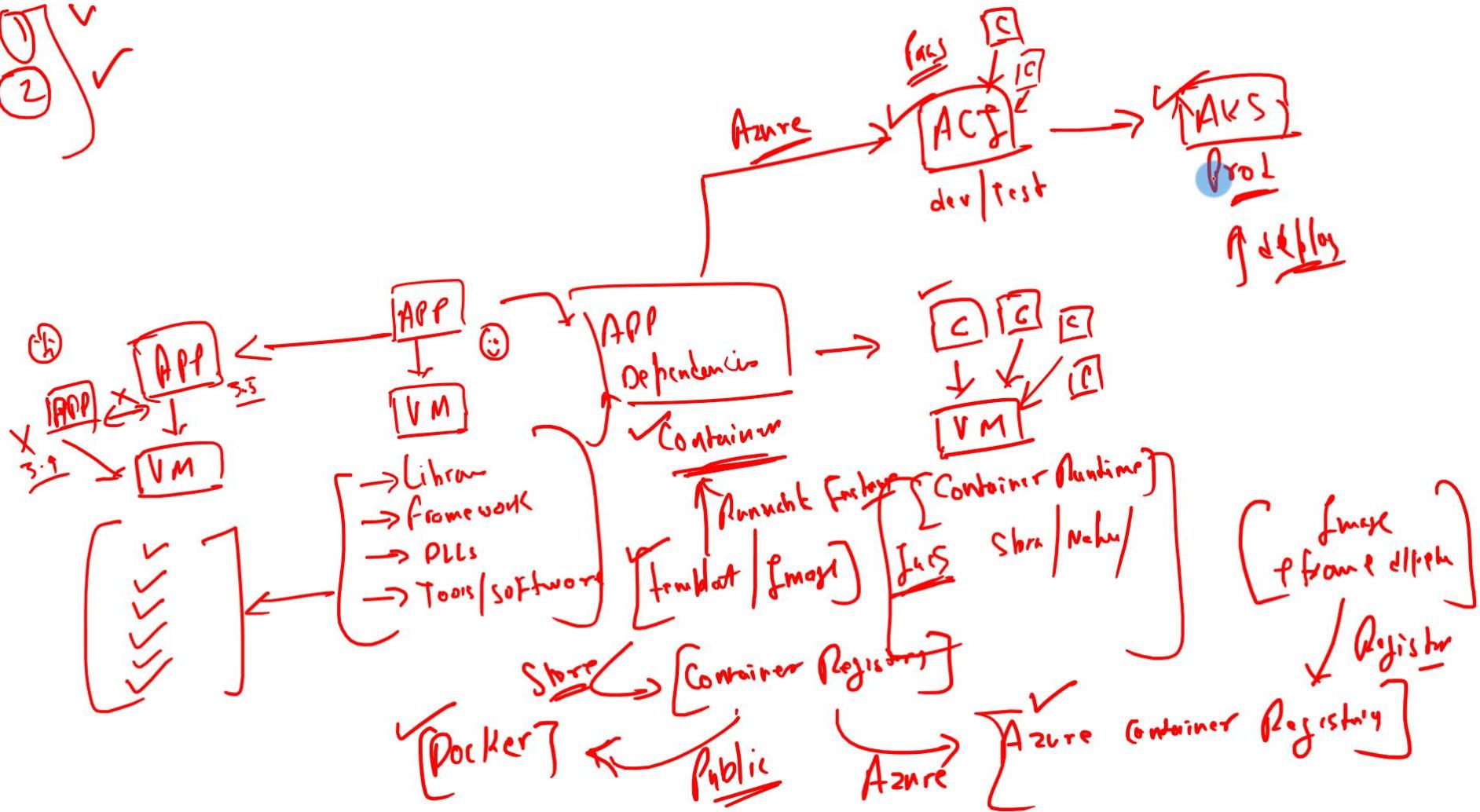


Security - App Service

- Deployment slots are live apps with their own hostnames.
- App content and configurations elements can be swapped between two deployment slots.
- Stage deployment slots allow you to test changes before deploying to production.
- Pre-warming a slot before deploying an app ensures that all instances of the slot are ready to go.
Deploying your app without downtime. No requests are lost due to traffic redirection.
- When pre-swap validation is not required, Auto Swap can be configured to automate the whole workflow.
- After a swap, the previously staged app is now the production app. To restore your “last known good site” if the changes swapped into production do not meet your expectations, simply perform the same swap.
- Automated swapping simplifies Azure DevOps scenarios that require no cold starts or downtime for app users. When auto swap from a source slot to production is enabled, App Service automatically swaps the app into production after it has warmed up in the source slot. Web apps on Linux don't support auto swap yet.

Containers

Wrap up an application into its own isolated package



Containers

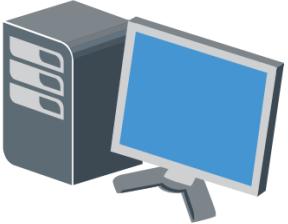
- **Problem Statement 1:** I can't share project with others because of dependencies on OS, framework, libraries and so on.
- **Problem Statement 2:** Need different machines to run three different Python-based applications that use of a different version of Python
- **Solution:** The simple solution is to create a container of your project in which you mention all the dependencies to run the project. Thus your project can be run universally on any computer having container runtime installed.
- *Containers are a way to wrap up an application into its own isolated package.*
- In a nut shell, Container is the modern era solution for transferring your projects to friends, family, colleagues, clients etc without worrying about their system configuration to run the project.
- Imp Features:
 - Portability: Deploy to diff environment
 - Consistency: will behave same each time
 - No maintenance related to infrastructure
 - Deployment and maintenance are efficient
 - Auto scaling



ACI vs AKS

Azure Container Instances (ACI) vs Azure Kubernetes Services

Hosting Options for Containers



Local Workstation



On-premises Servers



VMs in Azure



Azure Container Instances (ACI)



Azure Kubernetes Services (AKS)



Azure App Services

ACI vs AKS



Azure Container Instances (ACI)

- ACI is a service that lets you deploy containers on Azure without having to maintain or patch the environment.
- Basic web applications, Dev/Test scenarios, and batch processing are all supported by ACI.
- When you just need to run a few containers, it's a perfect option.
- Limited scalability and low availability
- Managed environment
- Only pay for containers
- Deployment is easy.

- Alternatively, For more complex container designs where you require additional control over the health and performance of your containers, you may utilize Azure Kubernetes Service (AKS).
- You can coordinate the deployment, update, and management operations for all of your containers using AKS.
- If you need to operate tens, hundreds, or even thousands of containers, the AKS Open source project could be a good fit.
- It's one tool in a class of tools called container orchestrators



Azure Kubernetes Service (AKS)

Azure Kubernetes Services (AKS)

- Azure's container management system
- Scale your application to meet demands by adding and removing container instances
- Monitor the deployed containers and resolving any issues that may come
- Groups of containers are called **Pods**
- Virtual machines are called **Nodes**
- Azure Container Registry pull



Azure Kubernetes Service (AKS)

Virtual Machine vs Containers

Virtual Machine vs Containers

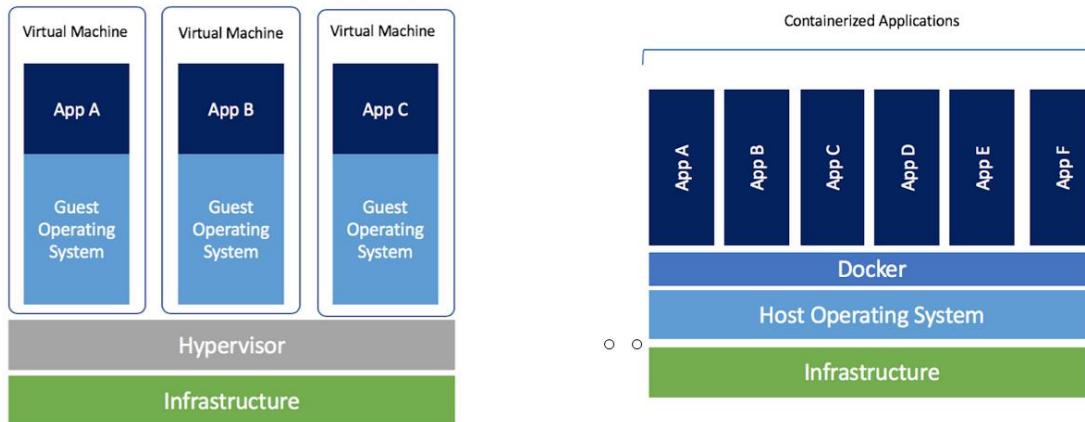


Image Reference: <https://www.docker.com/blog/containers-replacing-virtual-machines/>

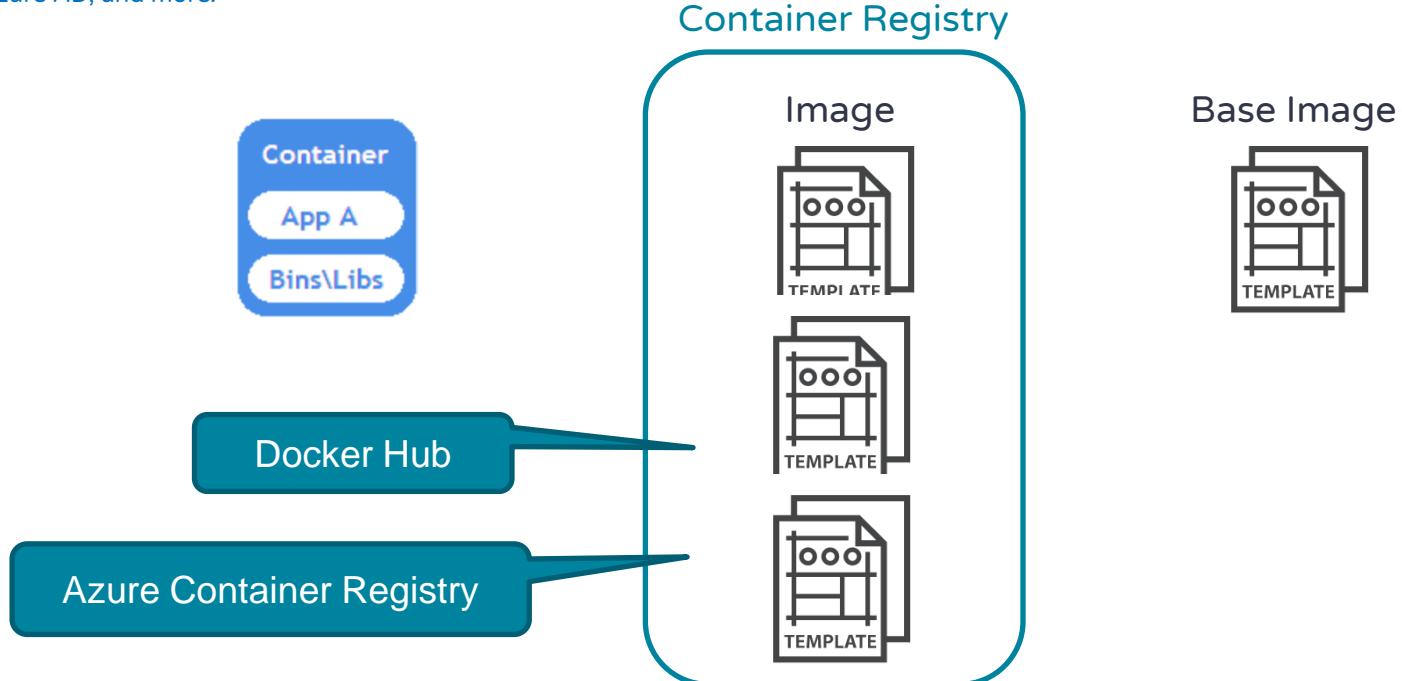
- Virtual machine contains a full copy of an operating system
- Virtual machine virtualizes the underlying hardware, meaning the CPU, memory, and storage
- Containers, on the other hand, virtualize the operating system.
- Containers smaller in size than a virtual machine and quicker to spin up because you're only waiting for the app to launch, not the operating system.

Docker & Azure Container Registry

Docker is an open source containerization platform

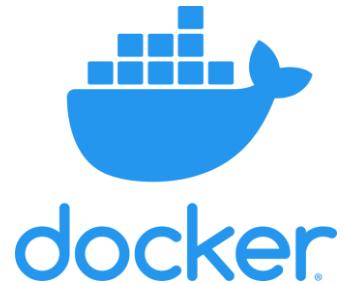
Azure Container Registry

- An image is a read-only template with instructions on how to create the container.
- Container is the runnable instance of the image.
- A container registry is a service that stores and distributes container images.
- Docker Hub is a public container registry on the web that serves as a general catalog of images.
 - Azure offers a similar service called **Azure Container Registry**, which gives customers complete control over their images, integrated authentication with Azure AD, and more.



What is Docker?

- A Docker container is a standard that describes the format of containers and provides a runtime for Docker containers.
- Docker is an open source project that automates the deployment of containers that can run in the cloud or on-premises.
- Docker is also a company that promotes and evolves the technology, and they work in collaboration with cloud vendors like Microsoft.
- The result from adopting docker, or container, is that application can be deployed or undeployed faster, start and stop faster, change to another “image” faster, process and do many things faster.
- Apps run the same, regardless of where they’re run
 - Any machine
 - No compatibility issues
 - Predictable behavior
 - Works with any language, any OS, any technology



Benefits of Azure Container instance (ACI)



Azure Container Instances (ACI)

Quick starting time - in seconds.

Bill-per second - only pay while the container is running

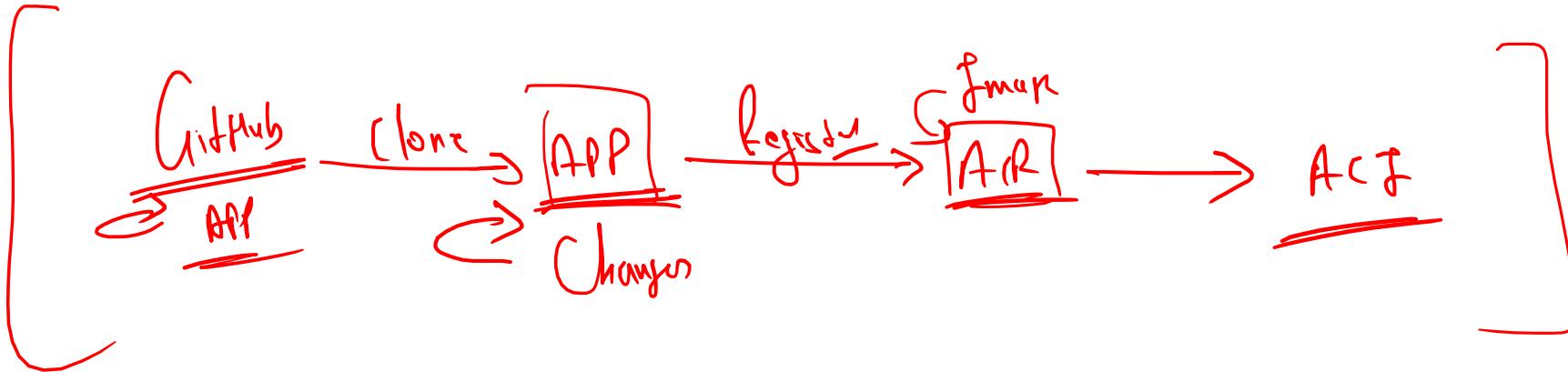
Highly secure - isolates your program like it would in a VM.

Custom sizes - define specific CPU cores and RAM.

Persistent storage - Azure file shares may be mounted straight to a container.

Linux and Windows - same API may schedule Linux and Windows containers.

Custom Images - ACR



Docker terminology

➤ Container.

- Container is an instance of a Docker image
- Represents single application, process, or service.
- Includes: application executable code, the runtime environment (such as .NET Core), system tools, settings.
- Can create multiple instances of a container from the same image

➤ Container image

- Refers to a package with all the dependencies and information required to create a container.
- Dependencies include frameworks and the deployment and execution configuration that a container runtime uses.
- Usually, an image derives from multiple base images that are layers stacked on top of each other to form the container's file system.
- An image is immutable once it has been created.

➤ Build

- Build refers to the action of building a container image based on the information and context provided by the Dockerfile.
- The build also includes any other files that are needed.

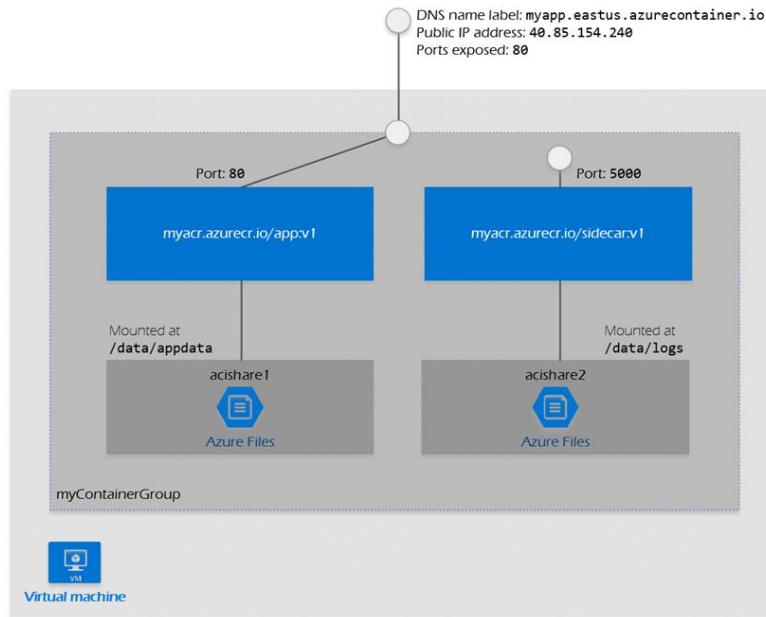
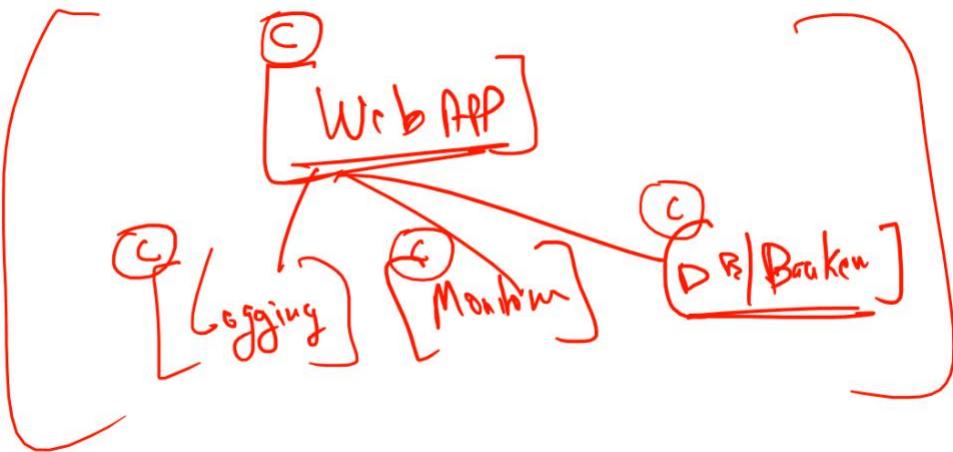
➤ Pull - Refers to the process of downloading a container image from a container registry.

➤ Push - Refers to the process of uploading a container image to a container registry.

➤ Dockerfile

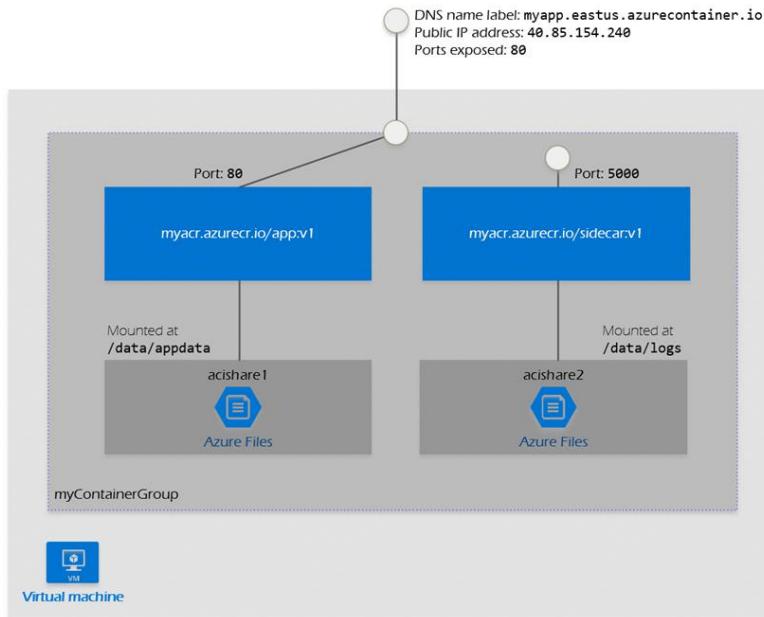
- Dockerfile refers to a text file that contains instructions on how to build a Docker image.
- The Dockerfile is like a batch script.
- The first line identifies the base image. The rest of the file includes the build actions.

Container groups



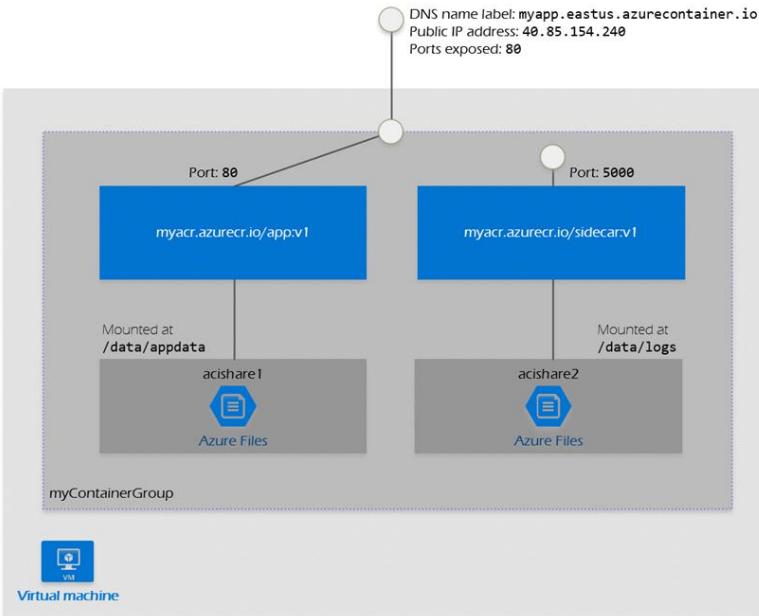
Container groups

- Container group is a collection of containers that get scheduled on the same host machine.
- Containers in a container group share a lifecycle, resources, local network, and storage volumes.
 - Similar in concept to a pod in Kubernetes.
- Multi-container groups currently support only Linux containers.
- Two common ways to deploy a multi-container group:
 - ARM Template – Also deploy additional Azure service resources (for example, an Azure Files share)
 - YAML file – only container instance, concise & recommended.
- Resource allocation



Container groups

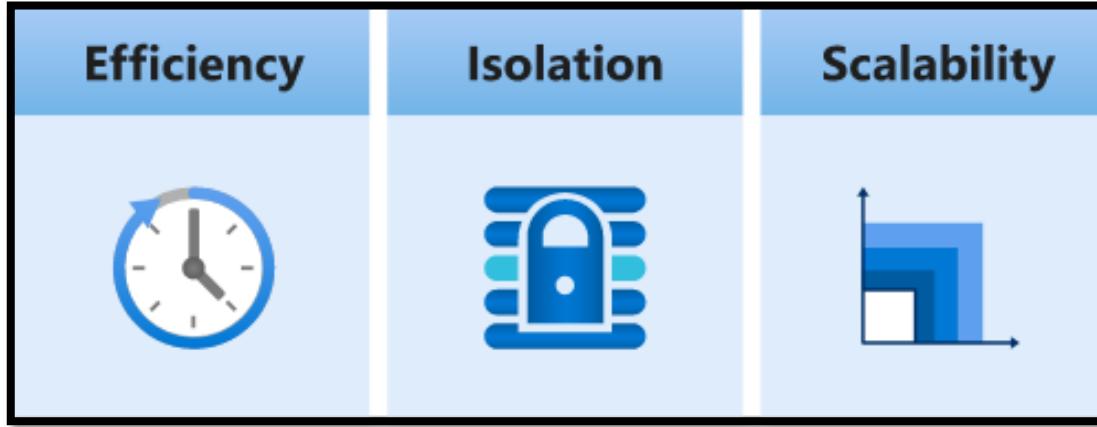
- Modify property in container – redeploy the group
 - All containers will be restarted
 - Will stay on same host system.
- Modify property that requires container deletion
 - OS type - Linux distribution
 - CPU, memory or GPU
 - Restart policy
 - Network profile



What is Kubernetes

open-source container orchestration system

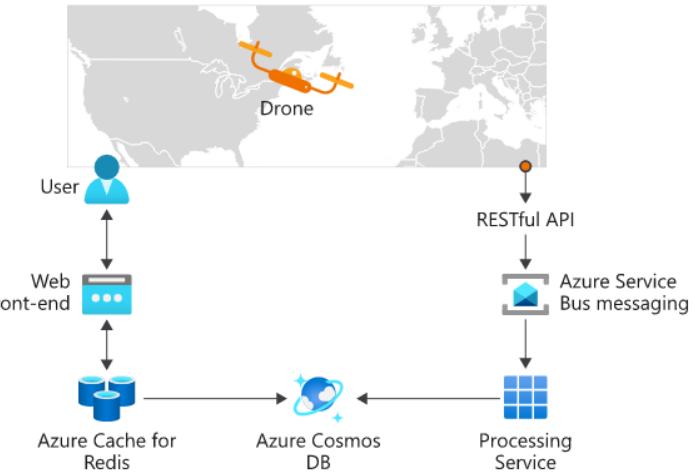
Containers



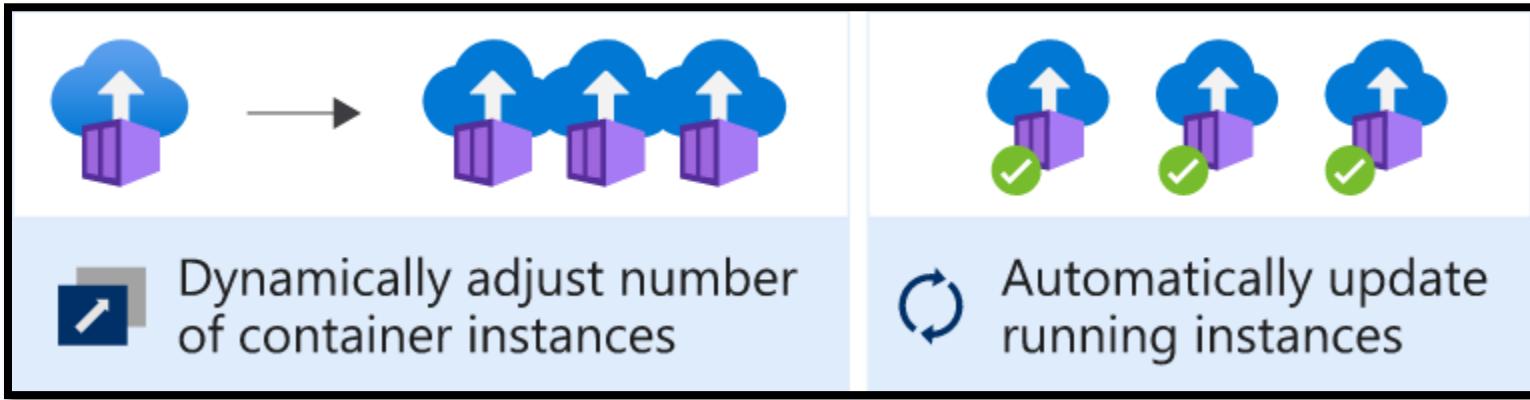
- Efficient use of hardware
- Secure to run multiple instances simultaneously on the same host without affecting each other
- Can scale out by deploying more instances.

Container management

- Challenges:
 - Configuring and maintaining load balancing
 - Network connectivity
 - Orchestrating the deployment process
- To make the management process easier, it's common to use a **container management platform**, such as **Kubernetes**.
- Container management is the process of organizing, adding, removing, or updating a significant number of containers.

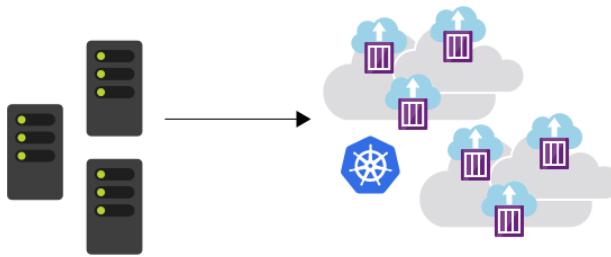


What is container orchestration?



Kubernetes

- Kubernetes abstracts away complex container management tasks, and provides you with declarative configuration to orchestrate containers in different computing environments.



- Benefits

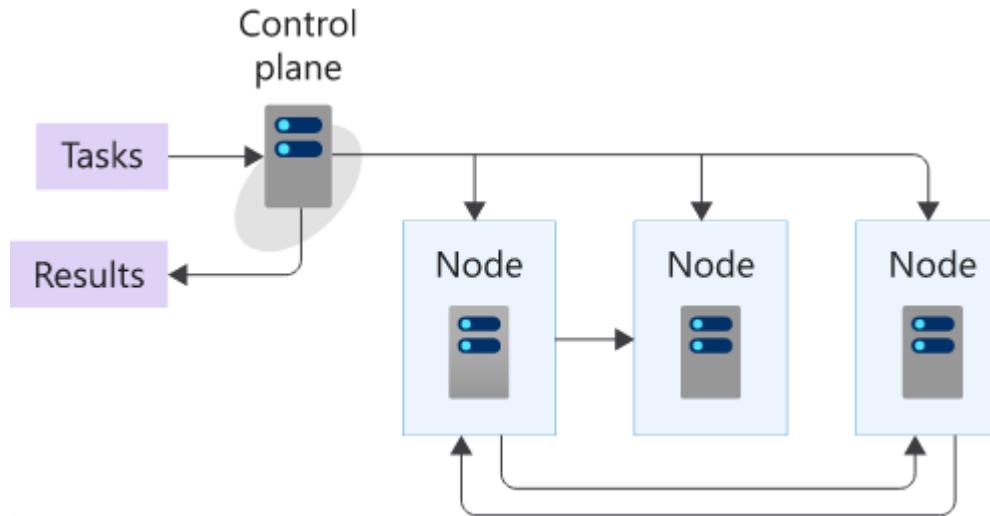
- Self-healing of containers. An example would be restarting containers that fail or replacing containers.
- Scaling deployed container count up or down dynamically, based on demand
- Automating rolling updates and rollbacks of containers.
- Managing storage.
- Managing network traffic.
- Storing and managing sensitive information, such as usernames and passwords.

Self-healing	Dynamic scaling	Rolling updates

Kubernetes architecture

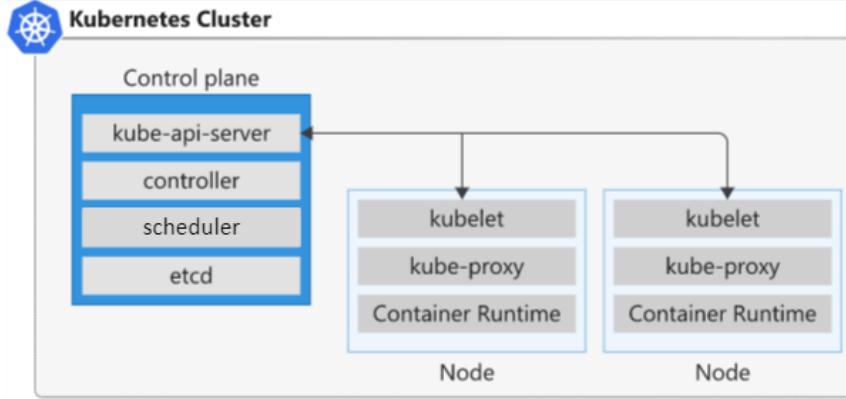
open-source container orchestration system

Computer cluster



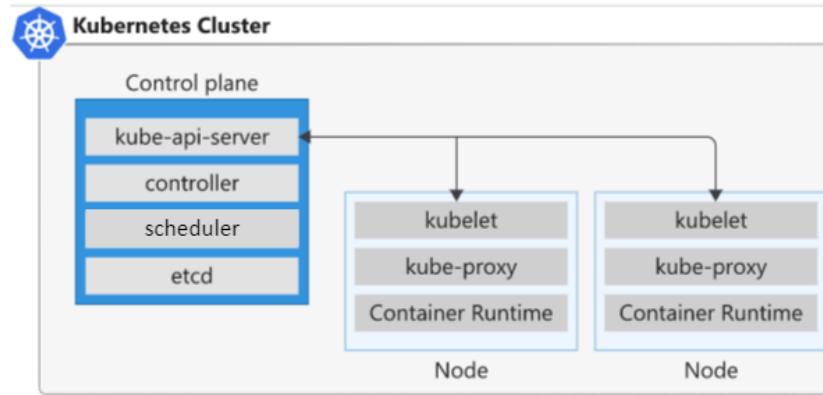
- **Master Node/ Control Planes** – that controls and manages the whole Kubernetes system
- **Worker Node** – that run the actual applications that you deploy.
- Both the control planes and node instances can be physical devices, virtual machines, or instances in the cloud.

Kubernetes architecture



- **API server** is like the front end to the control plane in your Kubernetes cluster.
 - All the communication between the components in Kubernetes is done through this API.
- **Scheduler** is the component that's responsible for the assignment of workloads across all nodes.
 - The scheduler monitors the cluster for newly created containers, and assigns them to nodes.
- **etcd** - key-value store
 - Stores the current state and the desired state of all objects within your cluster.
- **Controllers** track the state of objects in the cluster.
 - If the object's current state is not the desired state, the controller will intervene.

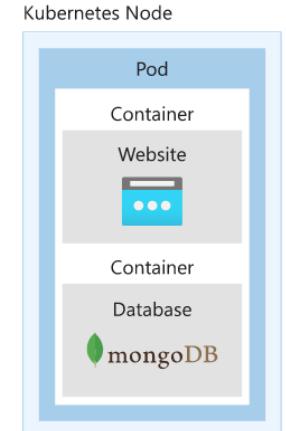
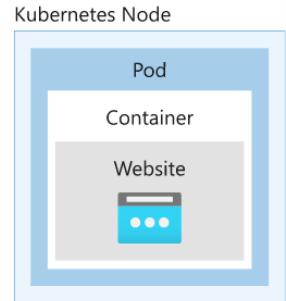
Kubernetes architecture



- **Kubelet** - monitors work requests from the API server
 - makes sure that the requested unit of work is running and healthy
- **kube-proxy** - handle routing and load balancing of traffic
 - responsible for local cluster networking
- **Container runtime** - runtime is responsible for fetching, starting, and stopping container images.

Kubernetes Objects

- kubectl is a command line interface for running commands against Kubernetes clusters.
 - Example : “kubectl get nodes” -> get the list of nodes running in your Kubernetes cluster
- Kubernetes pods
 - Represents a single instance of an app running in Kubernetes
 - A single pod can hold a group of one or more containers.
 - A pod includes information about the shared storage and network configuration, and a specification about how to run its packaged containers.
 - All container running within a pod will share the Node’s network with any other containers in the same pod
 - Containers within a pod can share files through volumes, attached to the containers
 - A pod has an explicit life cycle, and will always remain on the Node in which it was started.



Azure Kubernetes Service (AKS)

Deploy and scale containers on managed Kubernetes

Why we need Azure Kubernetes Service (AKS)

Challenges with Kubernetes

- You're responsible for finding the best solution for deployment, scaling, load balancing, logging, and monitoring.
- Need to understand concepts, such as microservices architecture.
- Kubernetes doesn't provide middleware, data-processing frameworks, databases, caches, or cluster storage systems.
- You're responsible for maintaining your Kubernetes environment.
 - Manually install the master and worker nodes
 - Need to consider high availability of the master, adding additional worker nodes, pathing, upgrades etc.
 - For example, you need to manage OS upgrades and the Kubernetes installation and upgrades.
 - You also manage the hardware configuration of the host machines, such as networking, memory, and storage.

Azure Kubernetes Service (AKS)

- Reduce these challenges by providing a hosted Kubernetes environment.
- Simplify the deployment and management of containerized apps in Azure.
- With AKS, you get the benefits of open-source Kubernetes without the complexity or operational overhead of running your own custom Kubernetes cluster.
- Microsoft manages the master node
- Microsoft Azure enterprise features are available to you.
- By offloading much of the responsibility for managing a Kubernetes cluster to Azure, it reduces the complexity and operational overhead.
- Takes care of important tasks for you, such as health monitoring and maintenance.



Azure Kubernetes Service (AKS)

Benefits of Azure Kubernetes Service (AKS)

Kubernetes version updates and patching are automated.

Cluster scaling is simple.

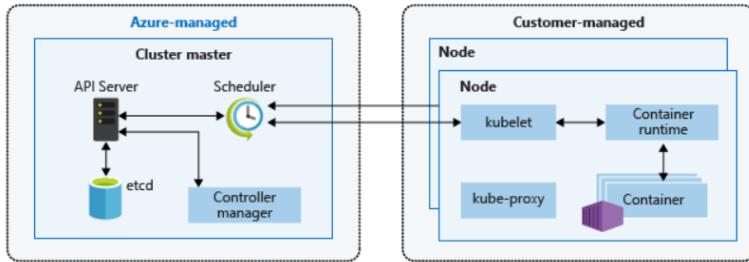
Hosted control plane that self-heals (masters)

Cost-cutting

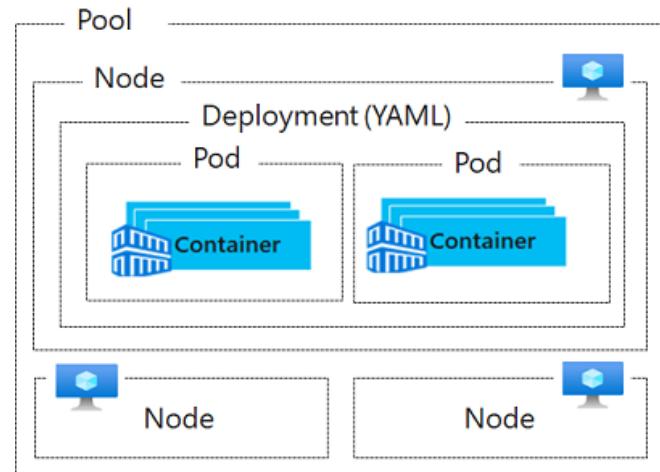


Azure Kubernetes Service (AKS)

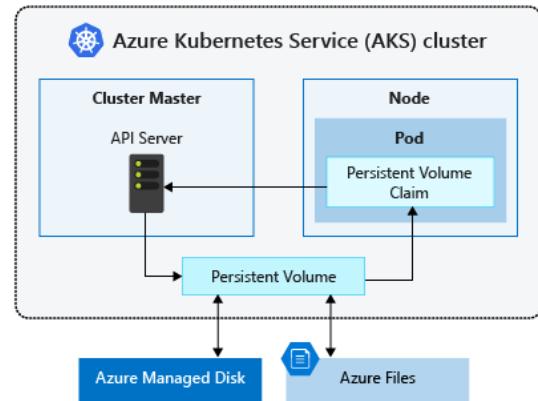
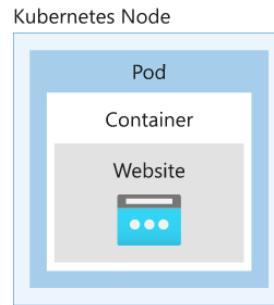
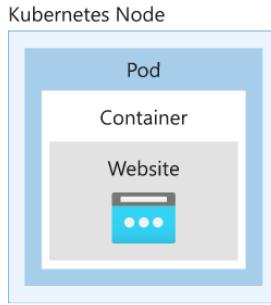
AKS terminology



- Pools are groups of nodes with identical configurations.
- Nodes are individual virtual machines running containerized applications.
- Pods are a single instance of an application. A pod can contain multiple containers.
- Container is a lightweight and portable executable image that contains software and all of its dependencies.
- Deployment has one or more identical pods managed by Kubernetes.
- Manifest is the YAML file describing a deployment.

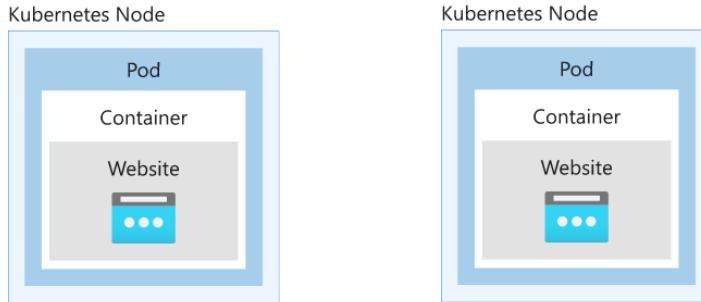


Storage in AKS

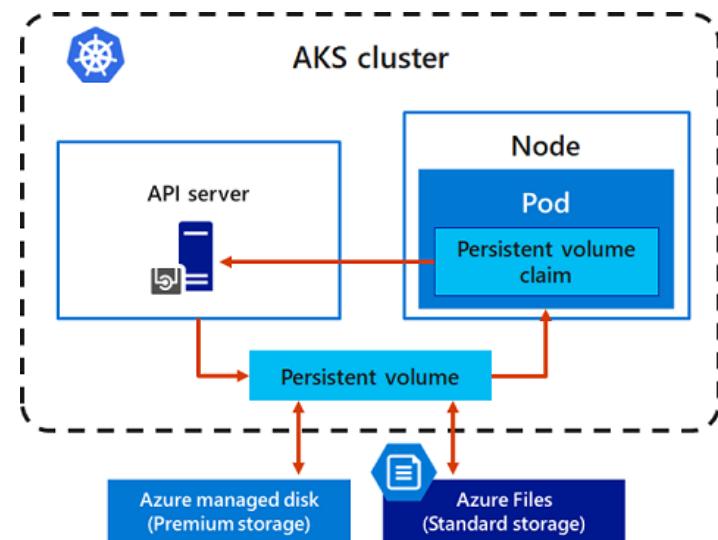


- Kubernetes typically treats individual pods as ephemeral, disposable resources.
- Multiple pods may need to:
 - Share the same data volumes.
 - Reattach data volumes if the pod is rescheduled on a different node.
- **Volume**
 - A volume represents a way to store, retrieve, and persist data across pods and through the application lifecycle.
 - You can manually create data volumes to be assigned to pods directly, or have Kubernetes automatically create them.

Storage in AKS



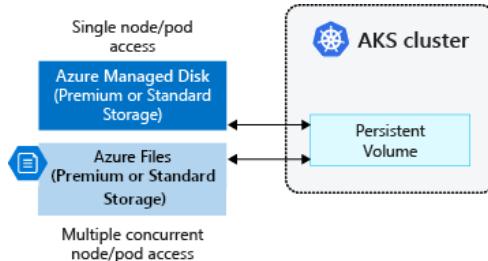
- Kubernetes typically treats individual pods as ephemeral, disposable resources.
- Multiple pods may need to:
 - Share the same data volumes.
 - Reattach data volumes if the pod is rescheduled on a different node.



Storage in AKS

➤ Volume

- Represents a way to store, retrieve, and persist data across pods and through the application lifecycle.
- Can be created manually or have Kubernetes automatically create them.

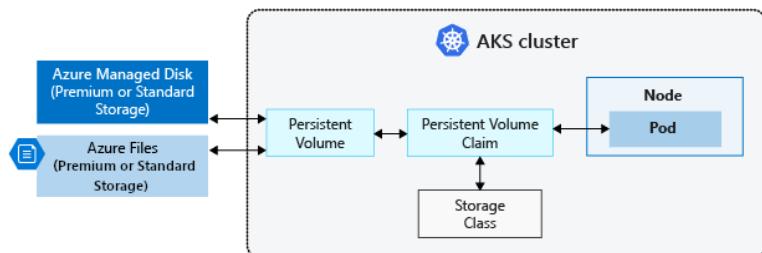


➤ Persistent volumes

- Storage resource created and managed by the Kubernetes API
- Can exist beyond the lifetime of an individual pod.
- Azure Disks or Azure Files
- Can be statically created by a cluster administrator, or dynamically created by the Kubernetes API server.

➤ Storage classes

- Define different tiers of storage, such as Premium and Standard
- Defines the *reclaimPolicy*

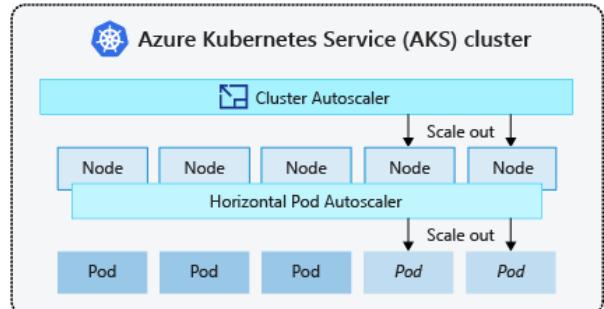
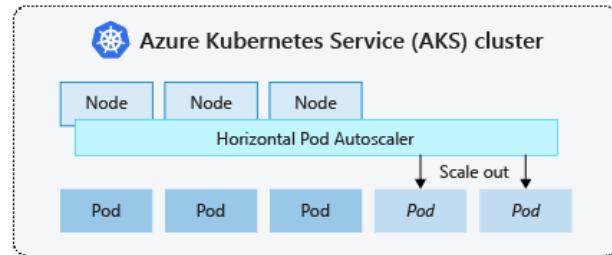


➤ Persistent volume claims

- A user's request for storage is called a **PersistentVolumeClaim**.
- Requests storage of a particular **StorageClass**, access mode, and size
- It looks like a pod. Node resources are consumed by pods, and **PersistentVolume** resources are consumed by **PersistentVolumeClaims**.
- Pods have the ability to request specific resource levels (CPU and Memory).
- Claims can specify a specific size and mode of access (for example, once read/write or many times read-only).

Scaling in AKS

- Scaling – as workload increase/decrease, you may need to increase/decrease infrastructure in terms of pods and nodes
- Manually scale
 - Scale Pods
 - Scale Nodes
- Horizontal pod autoscaler (HPA)
 - Monitor the resource demand and automatically scale the number of replicas
 - Define the minimum and maximum number of replicas that can run
 - Define the metric to monitor like CPU usage
- Cluster autoscaler
 - Adjusts the number of nodes based on the requested compute resources in the node pool
 - Scale out events – increase number of nodes because of node pool resource constraints
 - Scale in events – decreases the number of nodes because node pool has more compute resources than are required



Learning Objectives

Azure networking services

- In this module, you'll learn about the different Azure networking options and the scenarios in which each is appropriate.

- Virtual Network (VNet) and Subnets
- VPN Gateway and Vnet Peering
- Load Balancer and Application Gateway
- Content Delivery Network (CDN)
- ExpressRoute
- ExpressRoute vs VPN Gateway

IP Address – IPv4 vs IPv6

IP Address - IPv4 vs IPv6

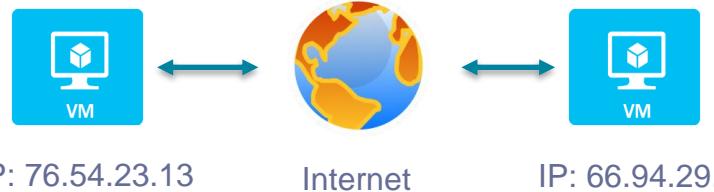
- A numeric address
- It's an identifier for a computer or device on a network
- Every device has to have an IP address for communication purposes.
- 2 types: IPv4 vs IPv6



IP Address - IPv4



- 32 bit numeric address written as four numbers separated by periods.
- Example: 66.94.234.03
- Each group of number separated by periods is called an **octet**.
- Number range in each octet is 0 to 255
- This address version can produce over 4 billion unique addresses



IP Address - IPv4

- Computers and network don't read IP addresses in this numeric format.
- They only understand binary format (1s and 0s)



66.94.29.03

01000010 . 01011110 . 00011101 . 00000011

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

8 Bit Octet Chart

Source: <https://docs.microsoft.com/>

IP Address - IPv6

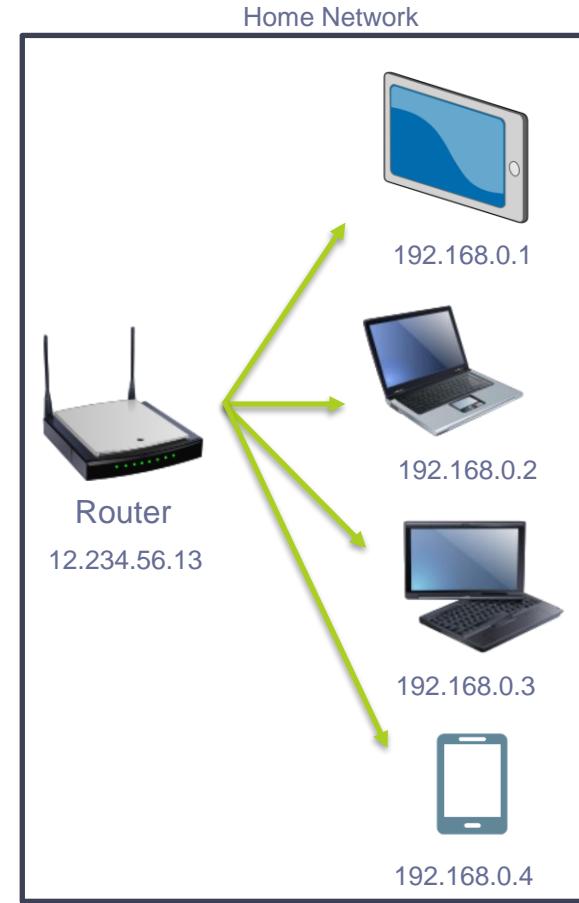
- 128 bit long new generation of IP addresses
- IPv6 address is represented as eight groups of four hexadecimal digits
 - Each group representing 16 bits[a]
 - The groups are separated by colons (:).
- An example of an IPv6 address is:
 - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Can produce 340 undecillion addresses
 - 340,282,366,920,938,463,463,374,607,431,768,211,456)
 - about 3.4×10^{38} (340 trillion trillion trillion) unique IPv6 addresses.

Public vs Private IP Address

Public vs Private IP Address

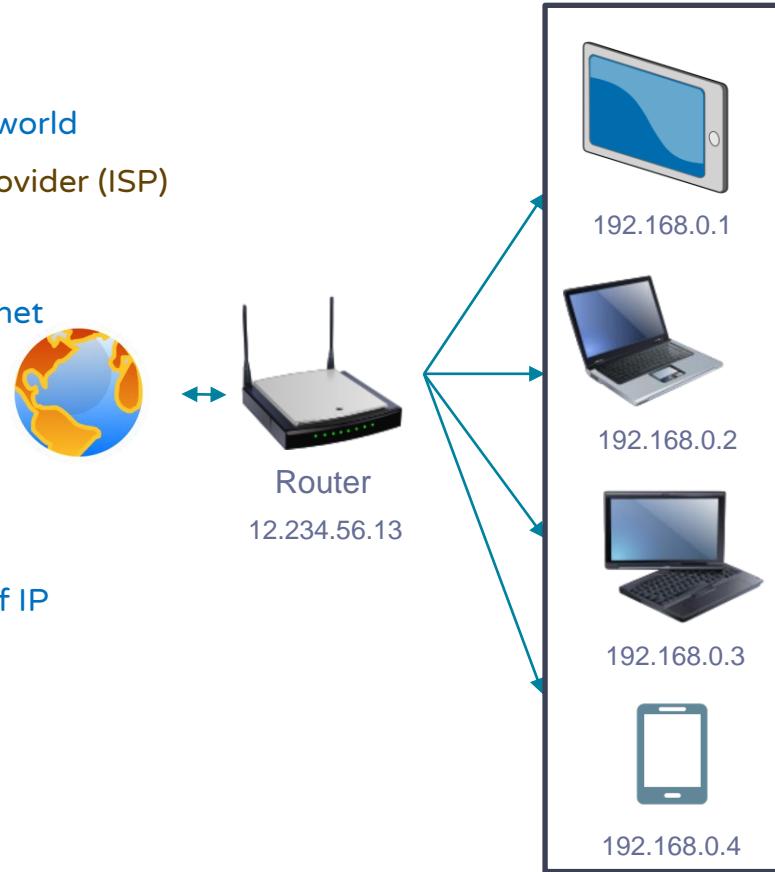
Public IP address for each device?

- More Expensive
- Unnecessary
- Waste of Public IP addresses



Public vs Private IP Address

- Public IP address
 - Public IP address are registered on the internet
 - Public IP address is Unique – no duplicate anywhere in the world
 - Assigned to your network router by your internet service provider (ISP)
- Private IP
 - Private IP addresses are not publicly registered on the internet
 - You can't access internet using a private IP address
 - Use internally – inside home, business etc.
 - Non-unique. Can be used on other private networks
 - DHCP is a service used in routers to assign private IPs
 - NAT (network address translation) is what translates a set of IP addresses to another set of IP addresses



Private IP Address

- Private IP address ranges can be used without registration in any number of private networks.
- For setting up private networks, three IP address ranges have been reserved by internet Assigned Numbers Authority (IANA)
 - Class A – for large organization
 - Class B – Medium size organization
 - Class C – home or small business

Class	Private IP address range	Subnet mask
A	10.0.0.0 – 10.255.255.255	255.0.0.0
B	172.16.0.0 – 172.16.31.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0

Public vs Private IP Address

Public IP address

- Unique
- Public registered on the internet
- Used externally
- Assigned by ISP
- Not free
- Not secure

Private IP Address

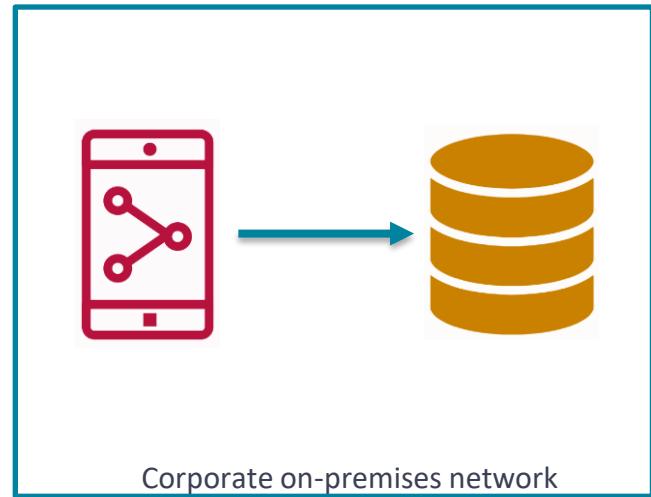
- Non-unique. Can be used on other private networks
- Not publicly registered
- Used internally
- Assigned by a router (DHCP service)
- FREE
- More secure

Virtual Network (VNet) and Subnets

Provision private networks, optionally connect to on-premises datacenters

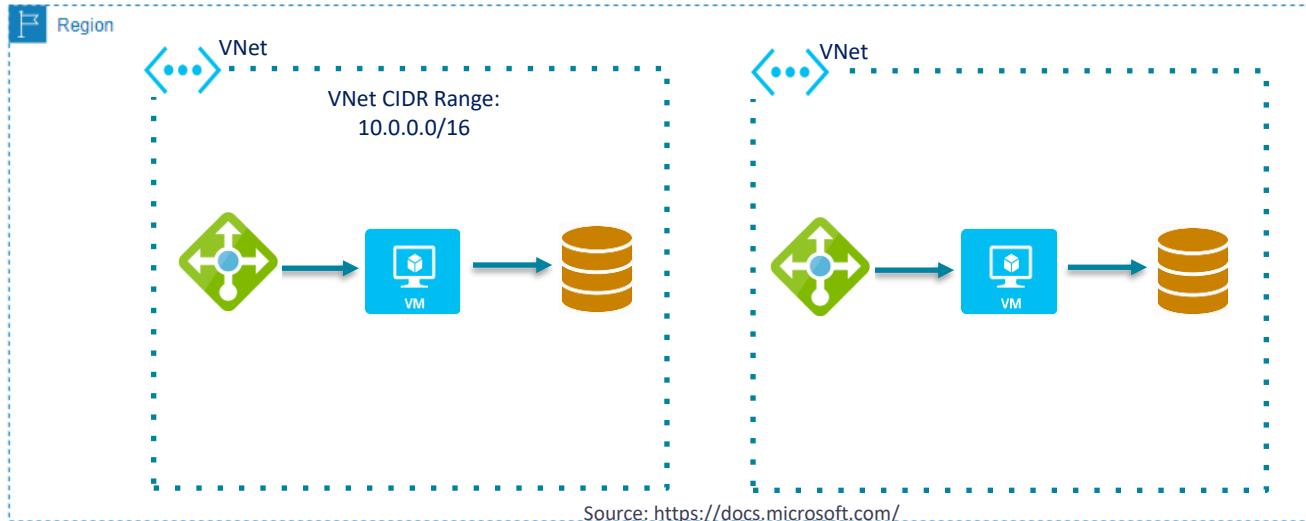
Need for Azure Virtual Network

- In a corporate on-premises data center network:
 - Nobody on the internet see the data exchange between the application and the database?
 - Nobody on the internet can directly connect to your database
 - You must first establish a connection to your corporate network before gaining access to your apps or databases.
- Corporate networks offer a secure internal network that safeguards your resources, data, and communications from unauthorized access.
- How can you build your own private cloud network?
 - Azure Virtual Network



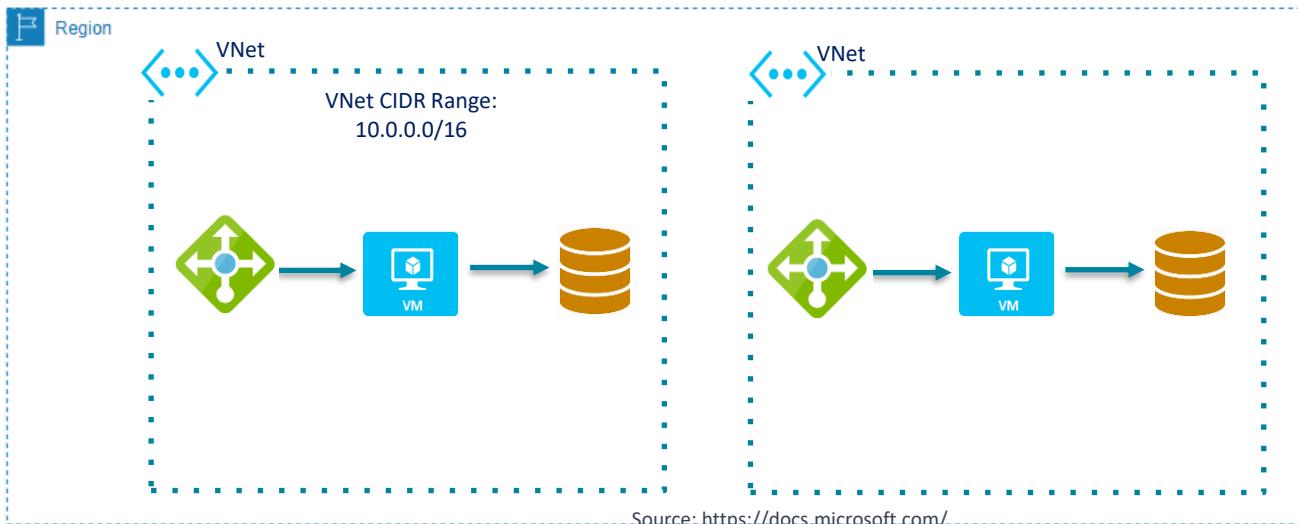
Azure Virtual Network

- Your own isolated network in Azure.
- Region can have multiple VNets but each VNet belong to same Region
- Within a VNet, network traffic is isolated (not visible) from network traffic in all other Azure VNet.
- You maintain complete control over all traffic entering and leaving a VNet.
- IP Address is a address of resource which ensures the traffic gets to the right server on the internet
- Every resource gets its own unique IP Address on that Vnet within the address space.
- Scaling – You can add more VNets or more addresses on existing VNet.



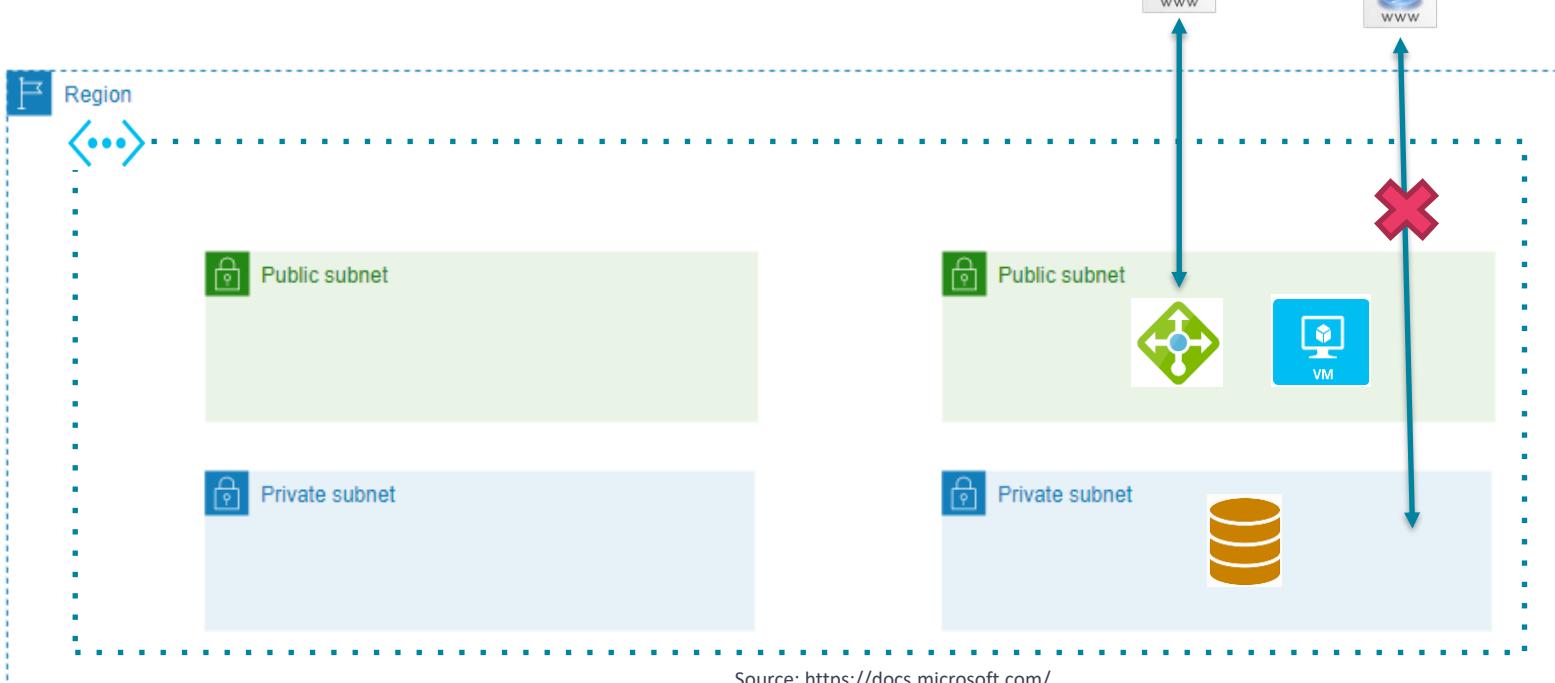
Need for VNet Subnets

- Each kind of resource has distinct access requirements.
- Elastic Load Balancers that are publicly available are accessible through the internet (public resources)
- Databases and App Server instances should be inaccessible from the internet.
- Only apps running inside your VNet should be able to access them (private resources).
- How do you partition public and private resources inside a VNet?



VNet Subnets

- Organize and group resources on subnets
- Separate public and private resources into distinct subnets
- Resources in a public subnet CAN be accessed from internet
- Resources in a private subnet CANNOT be accessed from internet, but resources in a public subnet can connect with resources in a private subnet.
- We can use network security groups to secure individual subnets



VNet Peering

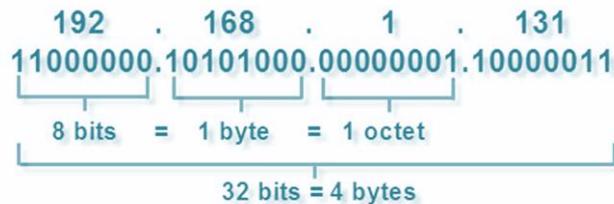
- Connect VNets from same or different regions (Global VNet peering)
- Allows for secure communication between VNets that are linked.
- Low Latency: Resources between diff VNets are connected using high bandwidth connections.
- Assemble them as though they were members of the same network
- Must not have CIDRs that overlap (IP address range)

Subnet Mask and CIDR

defines the range of IP addresses that can be used within a network

IPv4 Address

- IP address is a logical address that is used to uniquely identify a device on a network



	8 bits	8 bits	8 bits	8 bits
Decimal	0 - 255.	0 - 255.	0 - 255.	0 - 255
Binary	00000000 - 11111111.	00000000 - 11111111.	00000000 - 11111111.	00000000 - 11111111

What is the binary 10000011 in decimal?

	128	64	32	16	8	4	2	1		
Binary	1	0	0	0	0	0	1	1		
Decimal	128	+	0	+	0	+	0	+	1	= 131 Decimal

Subnet Mask

- In IP address = Network address + Host Address
 - 192.168.0.0
- The Subnet Mask specifies which part of the IP address corresponds to the network and which part corresponds to the host, by masking the network portion of the IP address.



	8 bits	8 bits	8 bits	8 bits
Class A:	Network	Host	Host	Host
IP Address	10.	0.	0.	15
Subnet Mask	11111111.	00000000.	00000000.	00000000

255. 0. 0. 0

	Network	Network	Host	Host
IP Address	172.	16.	0	.110
Subnet Mask	11111111.	11111111.	00000000.	00000000

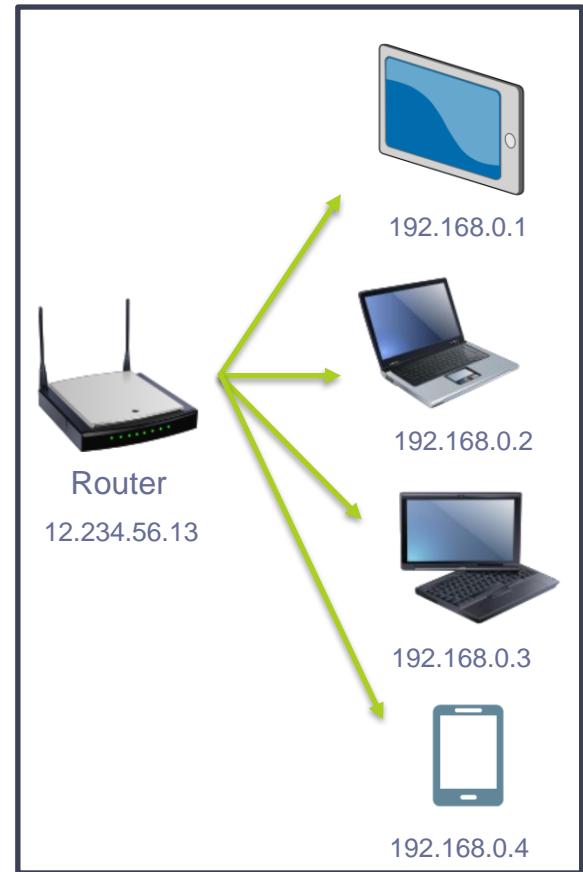
255. 255. 0. 0

	Network	Network	Network	Host
IP Address	192.	168.	1.	50
Subnet Mask	11111111.	11111111.	11111111.	00000000

255. 255. 255. 0

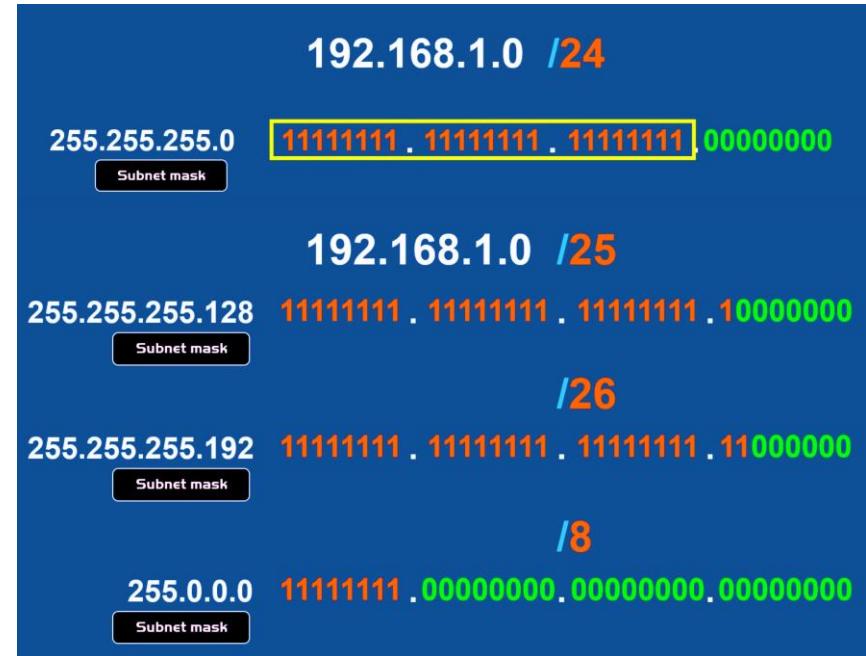


Home – Network Address



Subnet Mask and CIDR Notation

- Classless inter domain routing (Slash notation)
- It's a shorter way to write a subnet mask.
- “Slash” notation tells you how many bits are associated with Subnet Mask.



Network Interface Card (NIC)

NIC connects VM to the VNet

Network Interface Card (NIC)

- A network interface card (NIC) is a piece of hardware that allows a computer to connect to a network.
- Network Interface Card (NIC) also called:
 - Network Interface Controller
 - Network Adapter
 - LAN Adapter
- Can be:
 - Wired
 - Wireless
- A network interface enables an Azure Virtual Machine to communicate with internet, Azure, and on-premises resources.
- When you create VM using portal, one NIC with default setting created.
- IP address and NSG rules are attach with NIC
- You can create more than one NIC and attach to VM.

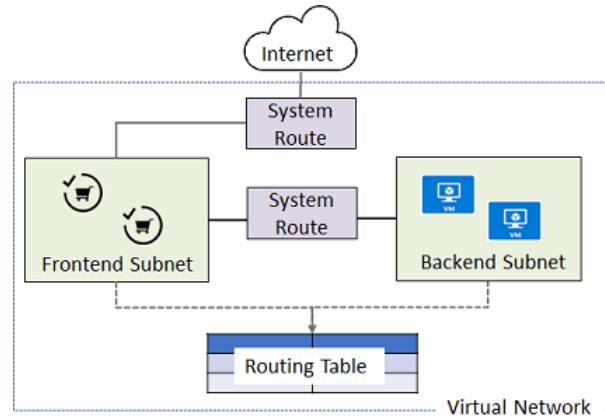


User-defined Routes (UDR)

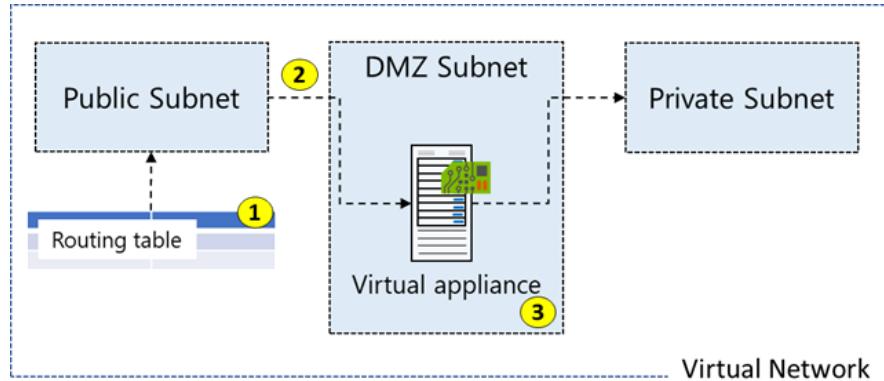
Route and Control the flow of traffic within Azure networks

System Route

- Routing: Process of finding/selecting a path for a traffic in one or across multiple networks
- Azure routing is setup by default
- Azure uses system routes to direct network traffic between virtual machines, on-premises networks, and the Internet.
- Information about the system routes is recorded in a route table.
- Routing tables are associated to subnets
- A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network.



User-defined network routes

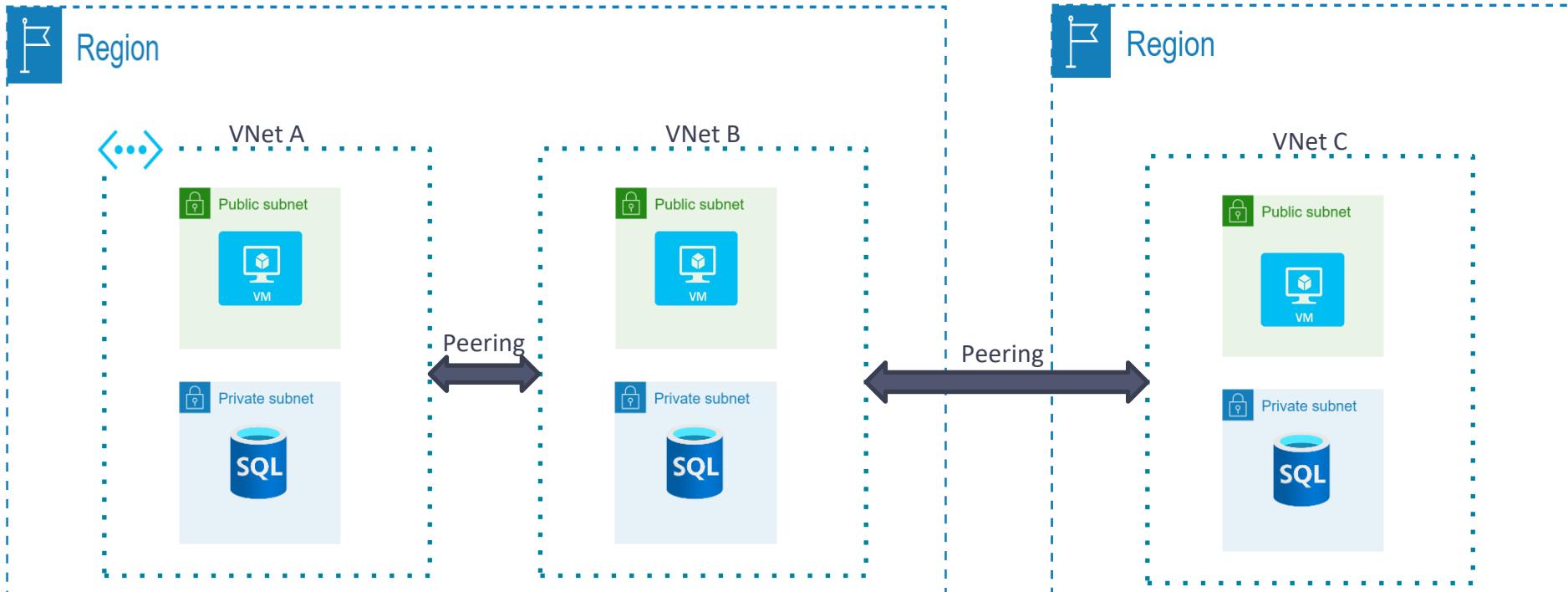


- Network Virtual appliance (NVA) – this is simply a specified optimized virtual machine for certain tasks.
- UDRs designed to override Azure default routing or add new routes
- Managed via Azure Route Table resource
- UDRs control network traffic by defining routes that specify the next hop (destination) of the traffic flow.
- The hop can be a virtual network gateway, virtual network, internet, or virtual appliance.
- Can be associated with more than one VNet subnets

Virtual Network Peering

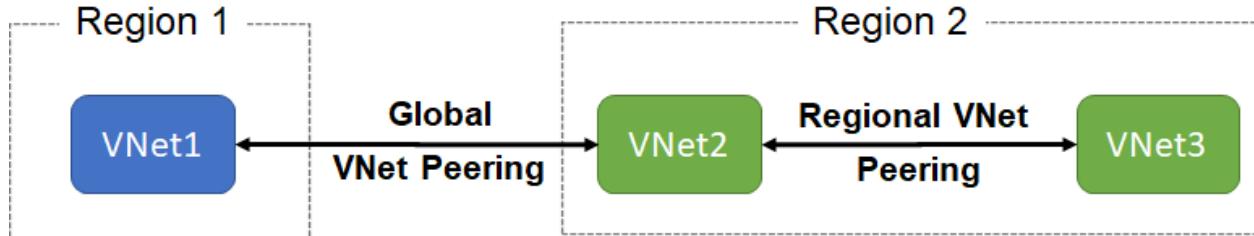
Connects two virtual networks in one region or across regions

VNet Peering



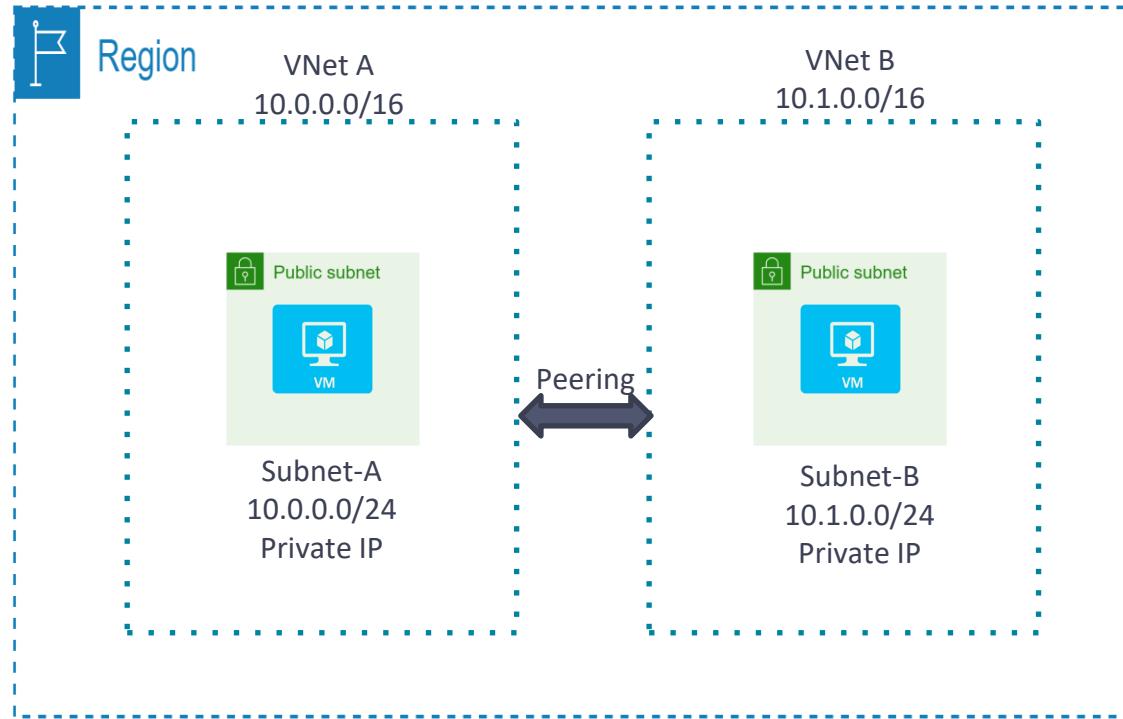
- Virtual networks are isolated with each other and have strong communication boundary.
- Azure network peering can connect two virtual networks located in the same region or across regions.

VNet Peering



- **Regional VNet peering** connects Azure virtual networks in the same region.
- **Global VNet peering** connects Azure virtual networks in different regions.
- The virtual networks can't have overlapping IP addresses.
- After peering, VMs across diff VNets can communicate using private IPs.
- **Benefits:**
 - **Private.** Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.
 - **Performance.** A low-latency, high-bandwidth connection between resources in different virtual networks.
 - **Seamless.** The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions.
 - **No disruption.** No downtime to resources in either virtual network when creating the peering, or after the peering is created.
- **Use case:** database failover, disaster recovery, or cross-region data replication

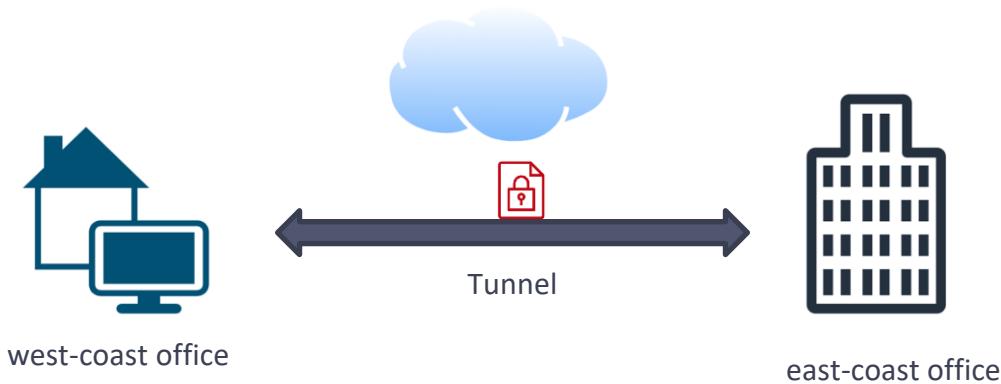
Demo: VNet Peering



VPN Gateway and Vnet Peering

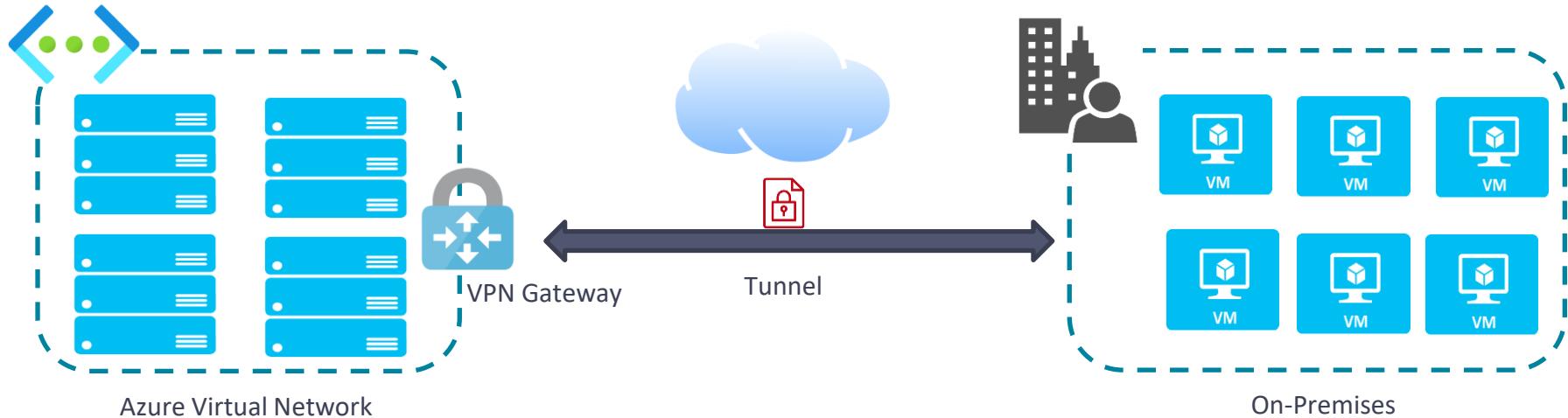
Connecting your infrastructure to the cloud

VPN (Virtual private network)



- Connect two or more trusted private networks to one another over securely an untrusted network (typically the public internet).
- Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.

VPN gateways



- Can connect Azure virtual network with On-premises network
- All transferred data is encrypted **in a private tunnel as it crosses the internet.**
- Azure VPN Gateway instances are deployed in Azure Virtual Network
 - Site-to-Site connection - Connect on-premises datacenters to virtual networks
 - Point-to-Site connection - Connect individual devices to virtual network
 - Multi-site connection – Connect more than one on-premises network to virtual network
 - Network-to-Network connection - Connect virtual networks to other virtual networks
 - We can also use “Network peering”

Network Connections



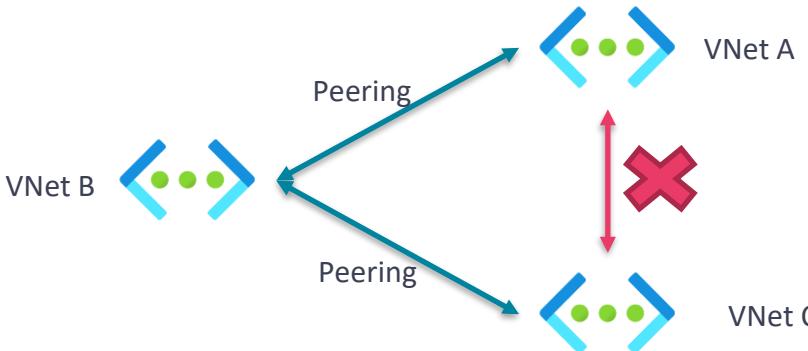
VPN Gateway vs Vnet Peering

- Vnet Peering
 - Connect VNets from same or different regions (Global VNet peering)
 - Allows for secure communication between VNets that are linked.
 - Low Latency: Resources between diff VNets are connected using high bandwidth connections.
- Which is best for you?
 - **VNet Peering** provides a low latency, high bandwidth connection useful in scenarios such as cross-region data replication and database failover scenarios. Since traffic is completely private and remains on the Microsoft backbone, customers with strict data policies prefer to use VNet Peering as public internet is not involved. Since there is no gateway in the path, there are no extra hops, ensuring low latency connections.
 - **VPN Gateways** provide a limited bandwidth connection and is useful in scenarios where encryption is needed, but bandwidth restrictions are tolerable. In these scenarios, customers are also not as latency-sensitive.

Service Chaining

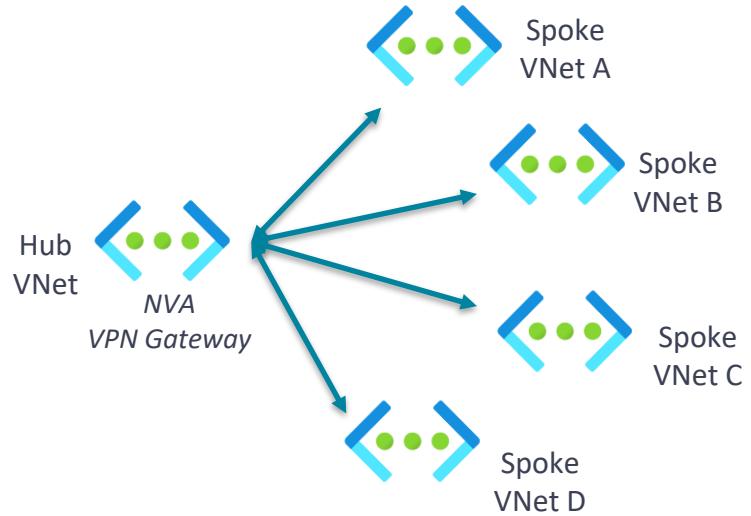
Enables you to direct traffic from one virtual network to a virtual appliance or gateway in a peered network through user-defined routes.

VNet Peering is nontransitive



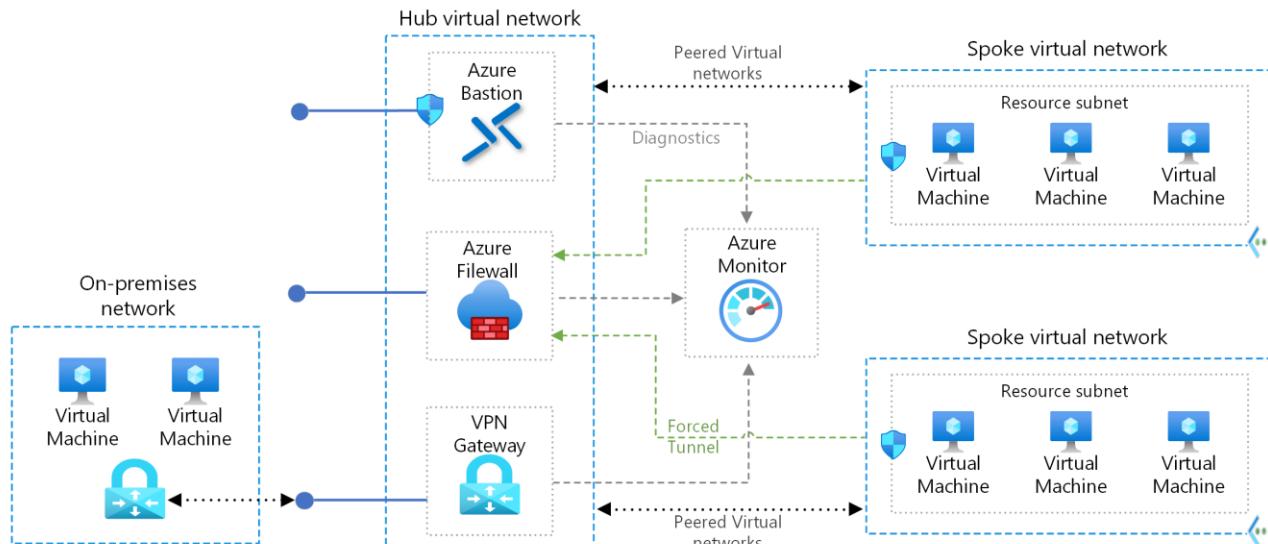
- VNet Peering is nontransitive
- Limit – 500 VNets peering per virtual network
- Configure user-defined routes and service chaining to provide the transitivity
- Implement a multi-level hub and spoke architecture.

Hub and spoke architecture



- Hub virtual network can host infrastructure components like the network virtual appliance or VPN gateway.
- All the spoke virtual networks can then peer with the hub virtual network.
- Traffic can flow through network virtual appliances or VPN gateways in the hub virtual network.

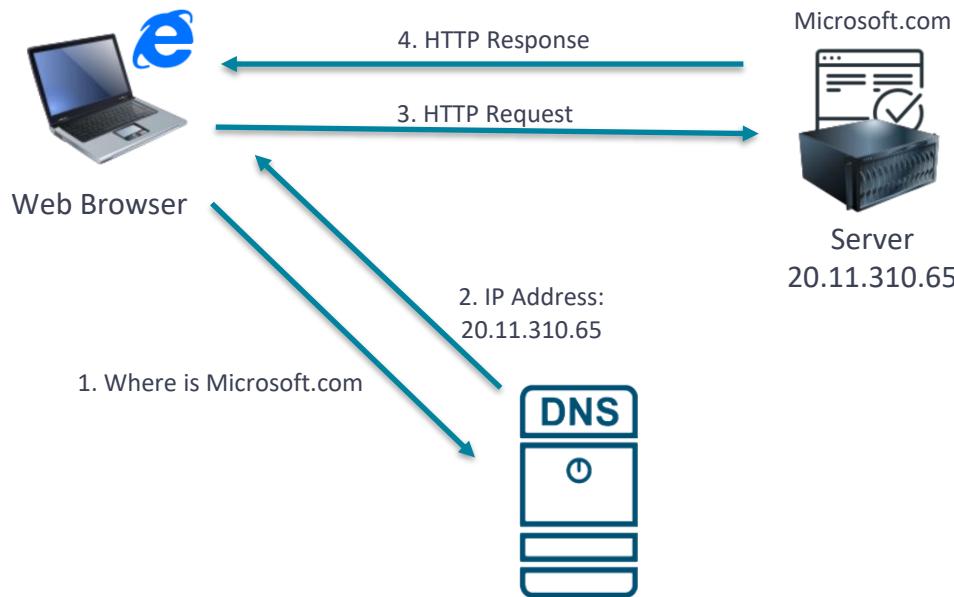
Hub and spoke architecture



DNS

Domain Name System

Domain Name System (DNS)



Domain Name System (DNS) translates (or resolve) a human-readable domain names, for example: www.wideworldimports.com, into a known IP address.

Laptop $\xrightarrow{\text{IE}}$ $(\cancel{\text{IP}} + \text{Port})$

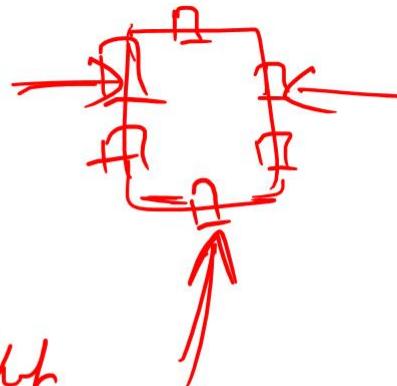
Wib Path

\downarrow

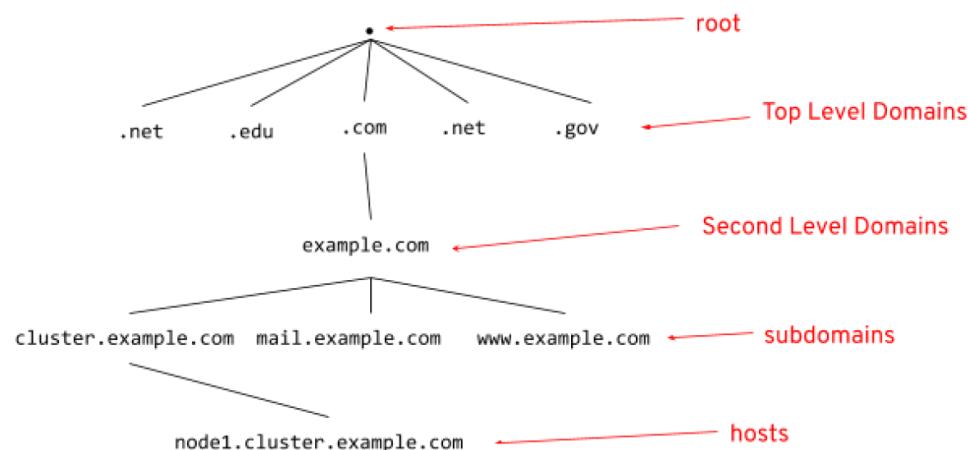
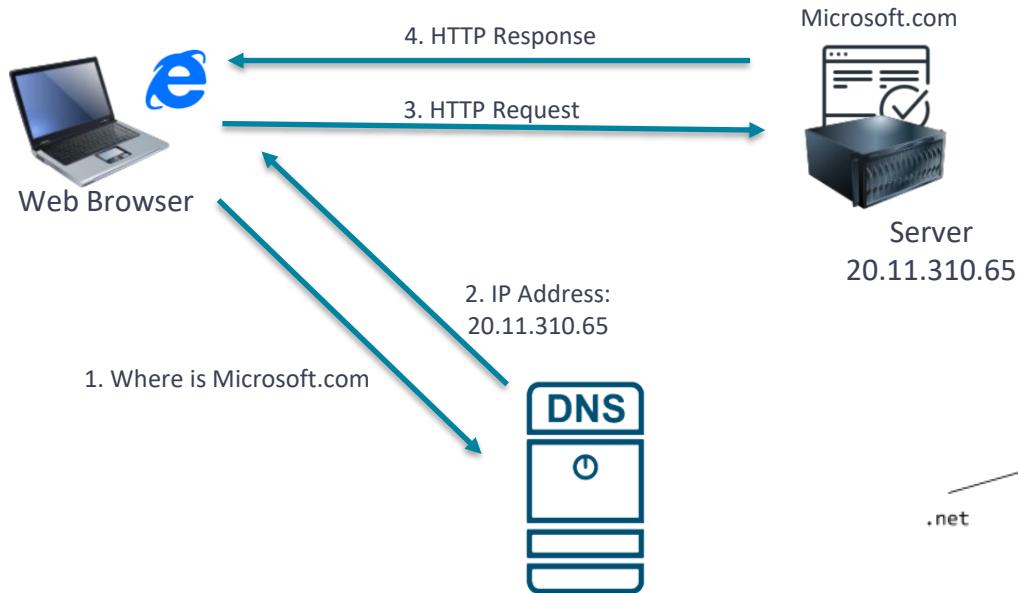
$\boxed{\text{VM} + \text{IIS}}$

$\boxed{\text{IP} + \text{Port Number} (80)}$

$\boxed{\text{VM} + \text{IIS}} \quad \boxed{\text{IP} + \text{Port Number} (80)}$ } South



Domain Name System (DNS)



Source: Redgate

Azure DNS

Domain Name System

Azure DNS



- Buy Domain Name (cloudgita.com)
- Manage DNS Server

Azure DNS

Internet-facing DNS domains

- Can NOT buy Domain Name
- Manage DNS Server

- DNS server is also known as a DNS name server, or just a name server.
- DNS uses a global directory hosted on servers around the world.
- Microsoft is part of that network that provides a DNS service through Azure DNS.

Source: Microsoft Docs



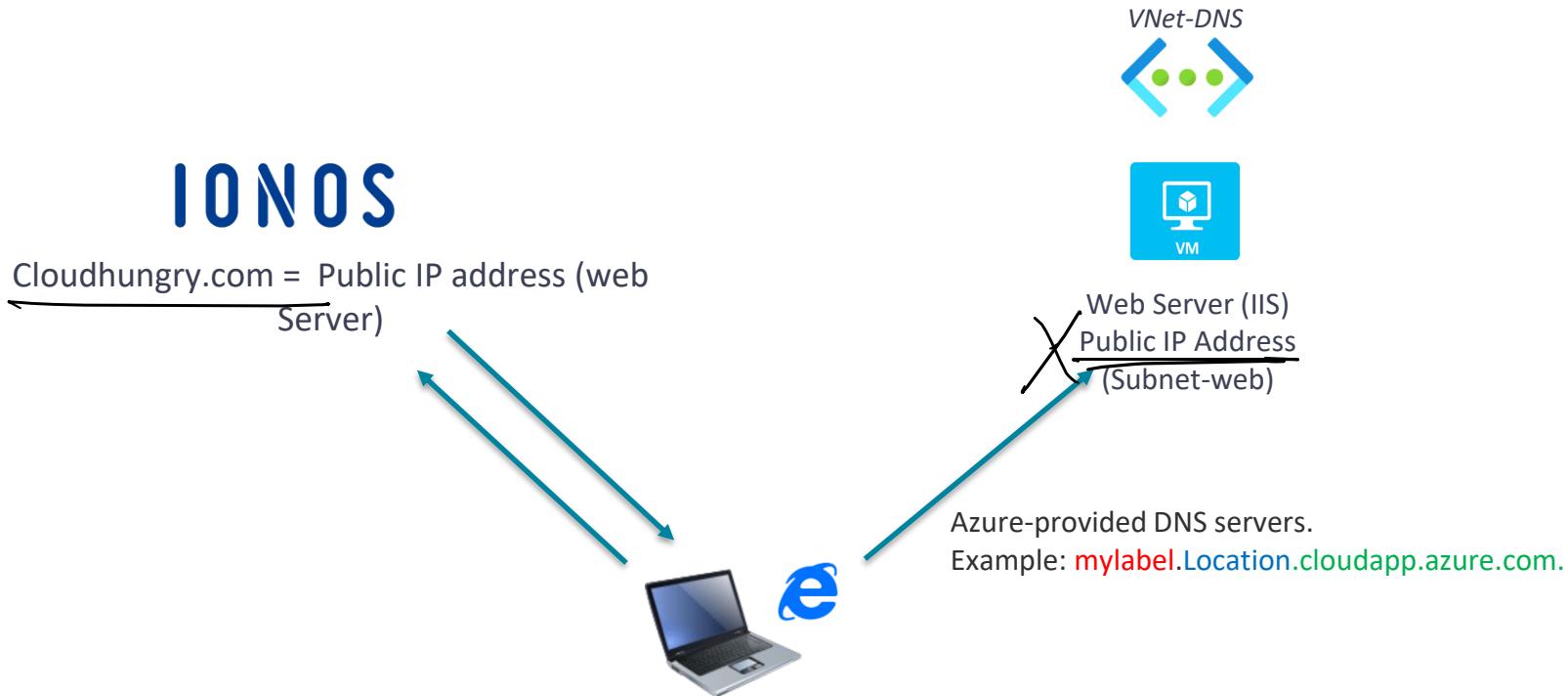
Install DNS Server



Azure Private DNS

Internal facing

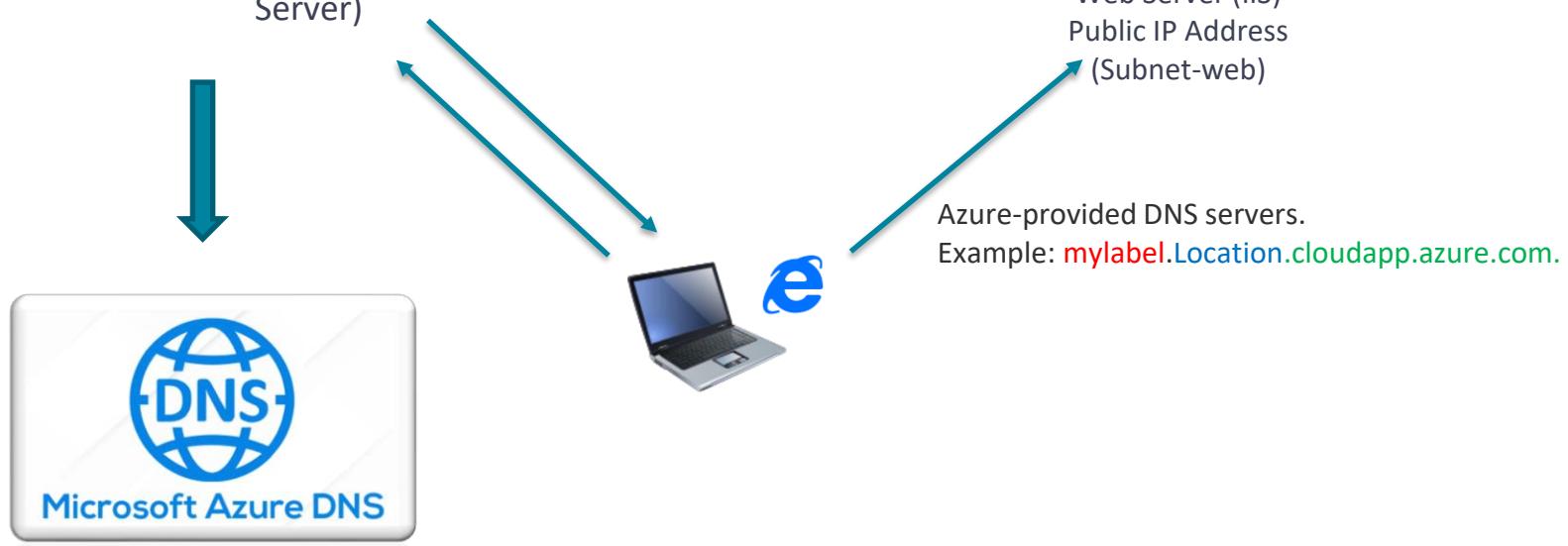
Demo: Configure DNS Server



Demo: Azure DNS Zone

IONOS

Cloudhungry.com = Public IP address (web
Server)

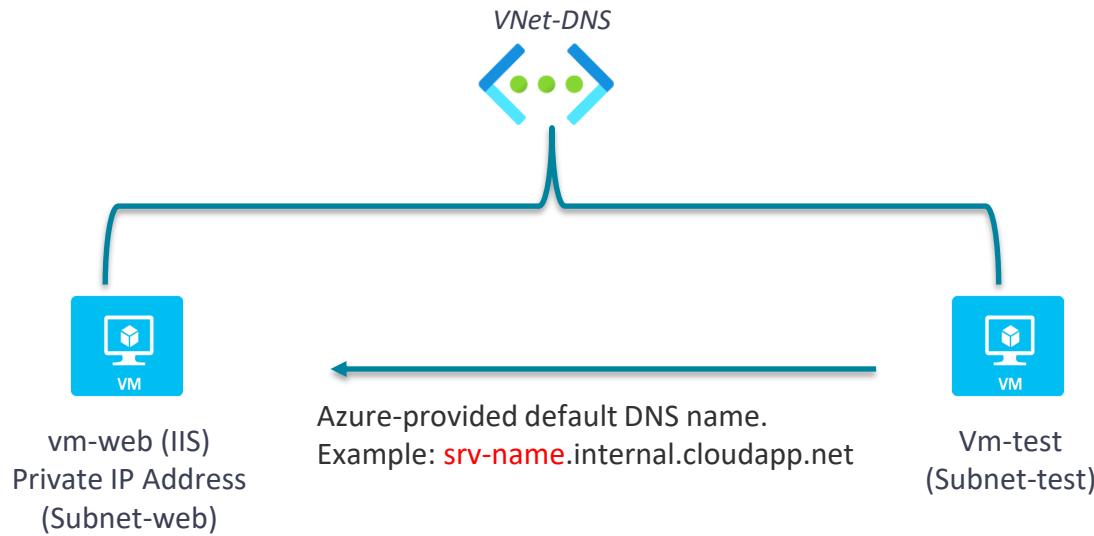


Azure DNS

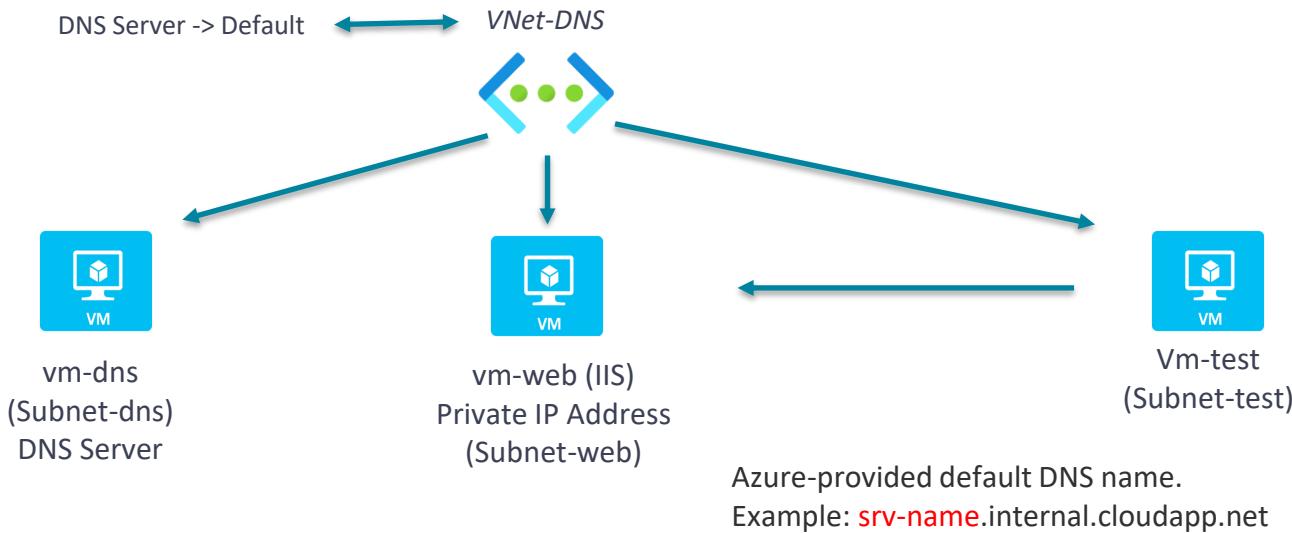
- Hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure.
- Domains can be hosted in Azure DNS for record management.
- Billing = no of DNS zones + number of DNS queries received
- Advantages:
 - DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers.
 - Each DNS query is answered by the closest available DNS server to provide fast performance and high availability for your domain.
 - Can be managed using Portal, PowerShell or CLI



Demo: Azure Internal Domain name

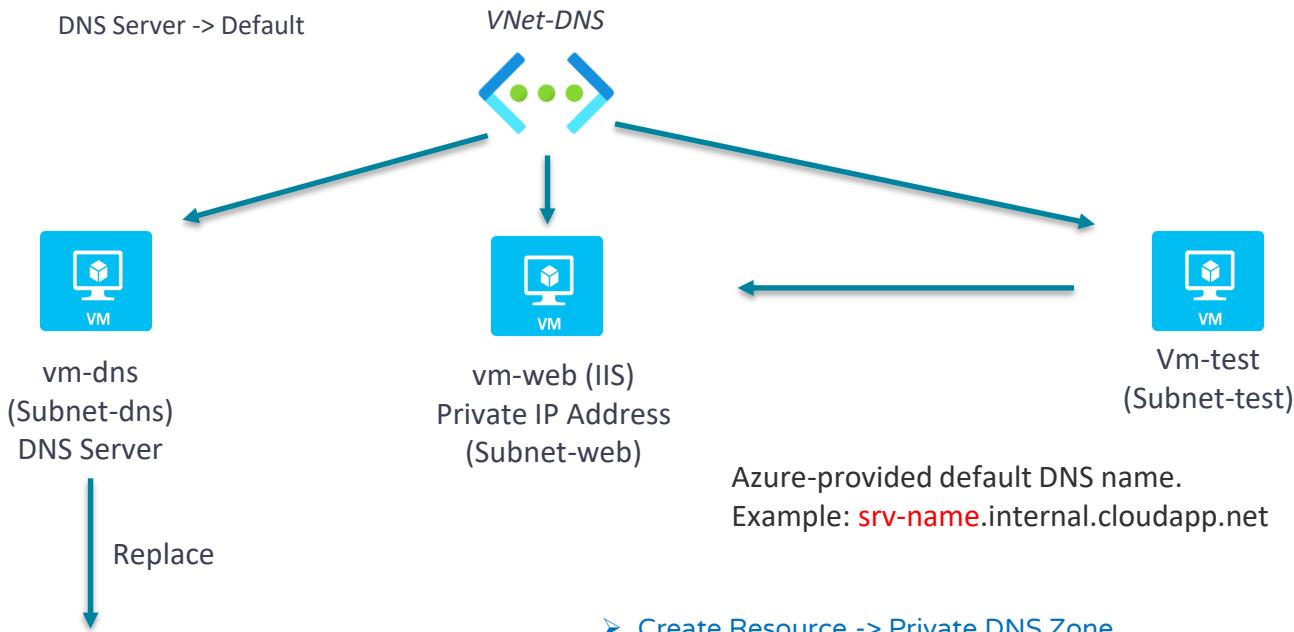


Demo: Host internal private DNS server



- Install DNS Server (Active Directory Domain Services)
- Promote the server to a domain controller
- Specify a root domain name – CloudGita.com
- Change VNet default DNS server to custom DNS Server we just created.
- Customize Azure provided domain names in vm-dns machine

Demo: Azure Private DNS

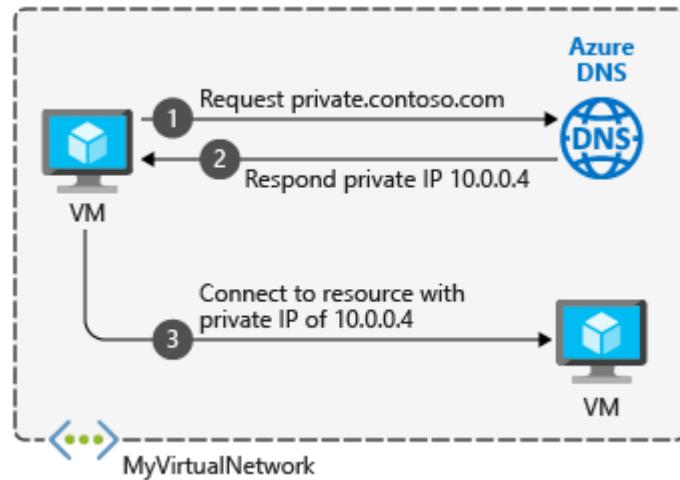


Azure Private DNS

Internal facing

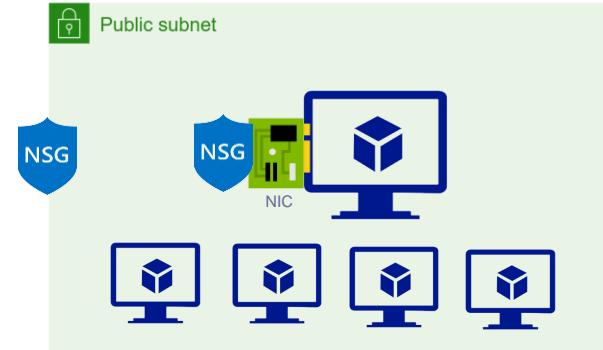
Azure Private DNS

- Azure Private DNS provides a reliable and secure DNS service for your virtual network. Azure
- Private DNS manages and resolves domain names in the virtual network without the need to configure a custom DNS solution.
- By using private DNS zones, you can use your own custom domain name instead of the Azure-provided names during deployment.
- A private zone can be linked to one or more virtual networks by the use of virtual networks links
- Auto-registration – This allows VM's to be automatically registered in the private DNS zone

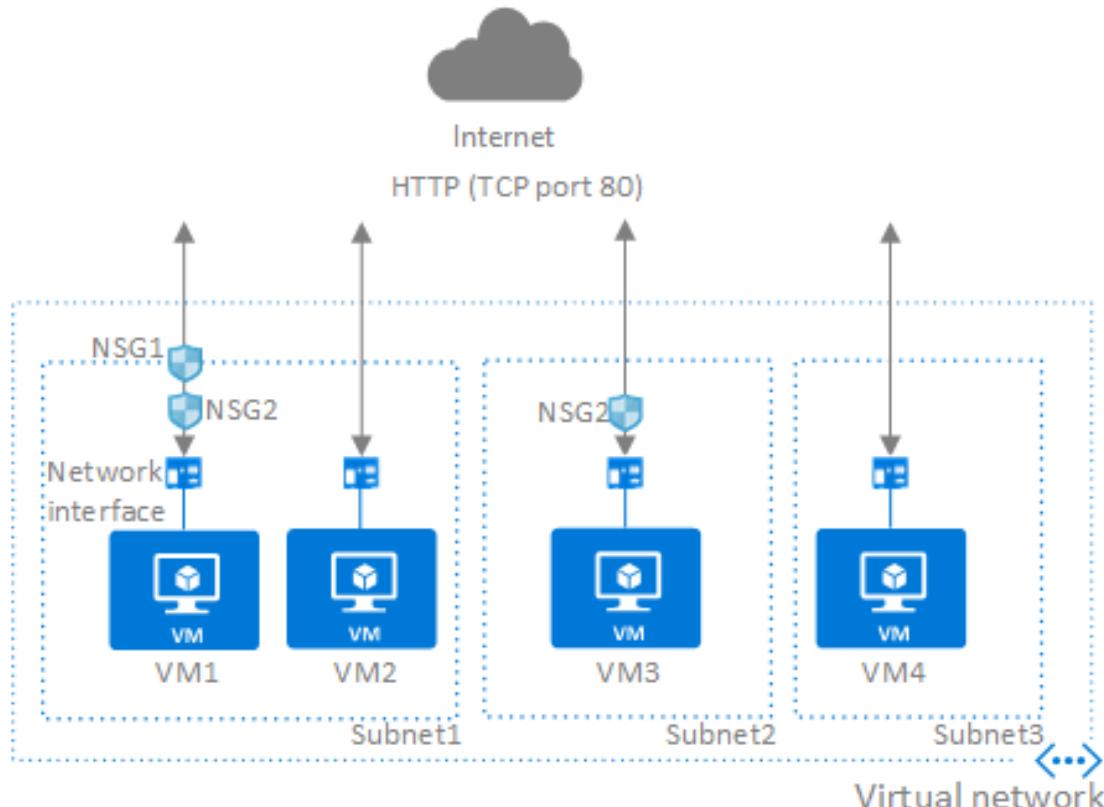


Network Security Group

- NSG can filter incoming and outgoing traffic.
- NSG can contain set of security rules which can allow or deny traffic
- NSGs is like internal firewall inside your Virtual network
 - Remember Azure firewall is an external firewall, outside your virtual network
 - NSG is a basic network filtering and does not have features like FQDN and threat intelligence.
- NSG can be associated to one or multiple subnets or network interface (NIC)
- You can't link NSG with VNet.
- OSI Layer 4 (5 properties or tuples)
 - Source and Destination IP address
 - Source and Destination port number
 - Protocol
- Priority – lower number, higher priority



Network Security Group

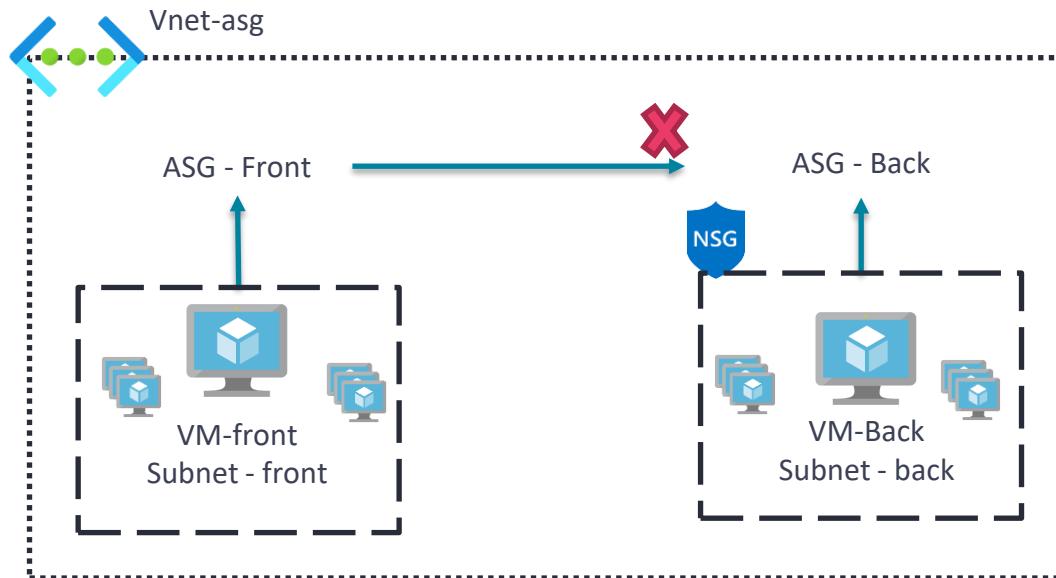


Application Security Group



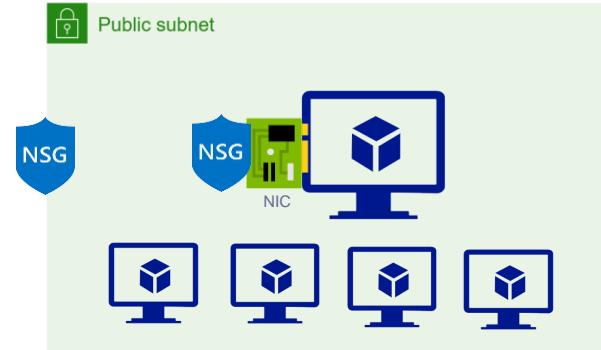
- Application security group allows you to group virtual machines and define NSG rules on that group.
- Don't need a manual maintenance of explicit IP addresses.
- ASGs introduce the ability to deploy multiple applications within the same subnet and also isolate traffic based on ASGs.
- If the VM is running more than one workloads, we can simply assign multiple ASGs.

Application Security Group



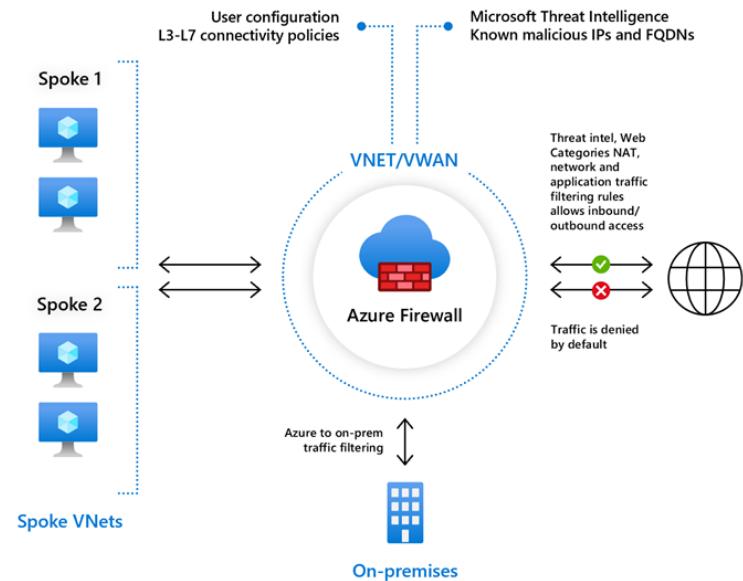
Network Security Group

- NSG can filter incoming and outgoing traffic.
- NSG can contain set of security rules which can allow or deny traffic
- NSGs is like internal firewall inside your Virtual network
 - Remember Azure firewall is an external firewall, outside your virtual network
 - NSG is a basic network filtering and does not have features like FQDN and threat intelligence.
- NSG can be associated to one or multiple subnets or network interface (NIC)
- You can't link NSG with VNet.
- OSI Layer 4 (5 properties or tuples)
 - Source and Destination IP address
 - Source and Destination port number
 - Protocol
- Priority – lower number, higher priority



Azure Firewall

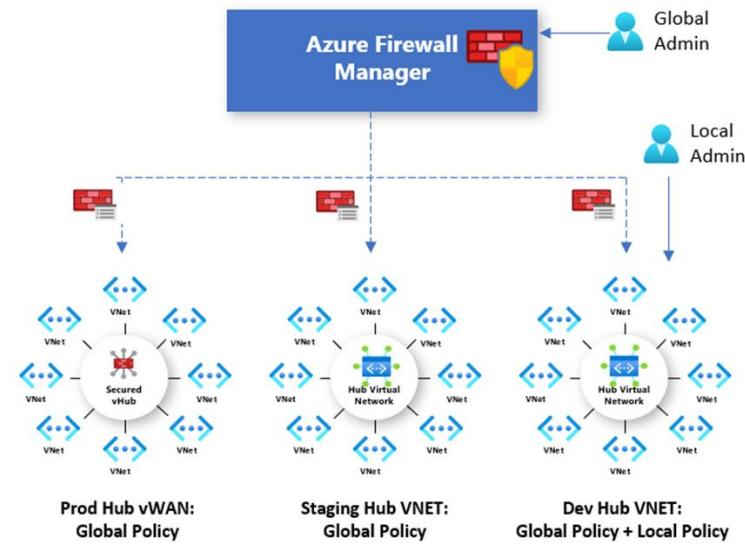
- Managed, network security service that protects your Azure Virtual Network resources.
- Highly available and unrestricted scalable.
- Fully integrated with Azure Monitor for logging and analytics.
- Just like with NSGs, your Azure Firewall rules can apply inbound and outbound access.
- Azure Firewall goes from OSI layer 3 all the way up to layer 7
 - NSG operates at OSI layer 4
 - Firewall can also deal with DNS names, as well as ports, protocols, and IP addresses.
- Azure Firewall can function in a hybrid cloud
 - All traffic that's going from your Azure infrastructure to on-premises has to go through the Azure Firewall
- The Azure firewall uses a statically assigned public IP address.



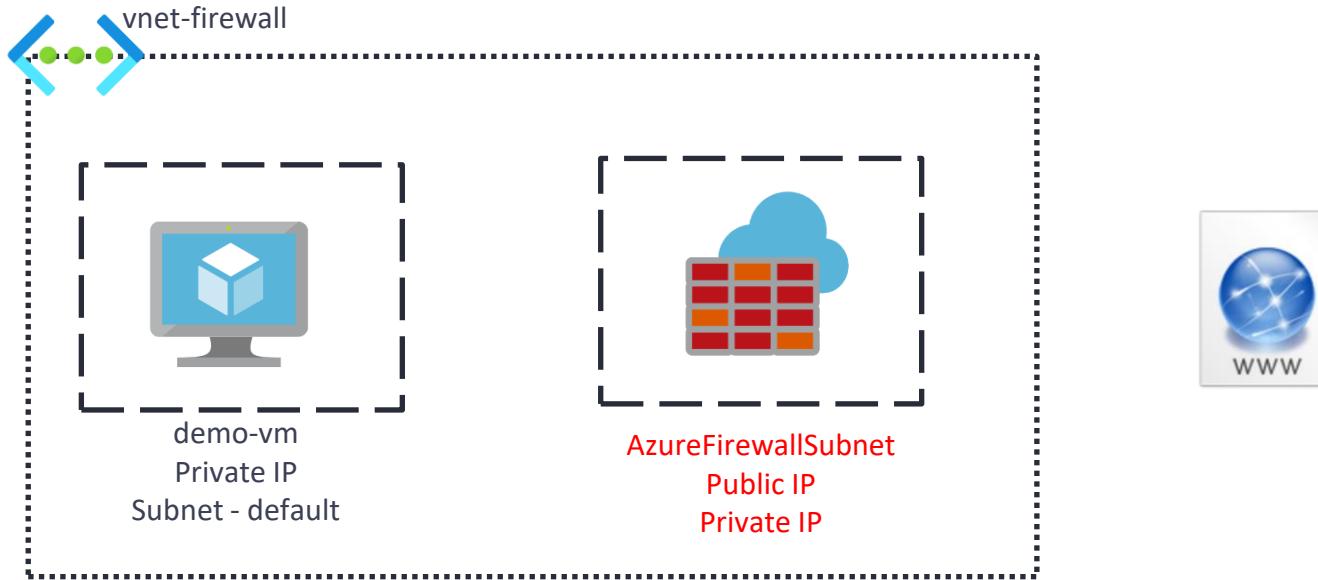
Azure Firewall Manager

➤ Azure Firewall Manager

- Centrally manage Azure Firewalls across multiple subscriptions.
- Rule sets can be shared across multiple Azure Firewall instances.
- Can integrate with third-party services, like iboss, Zscaler, and Check Point, to provide additional firewall or enterprise class firewall functionality
- Can also integrate with the virtual WAN concept.



Demo: Azure Firewall



Azure Firewall Rules

- By default, Azure Firewall blocks all traffic, unless you enable it.
- You create Rules
- Rule collection: zero or more Rules. They are of type NAT, Network or Applications. All rules in collection must be of same type.
- Rule Collection Group: zero or more Rule collection. Multiple collection types can be in one group.
- With Firewall Policy, rules are organized inside Rule Collections and Rule Collection Groups.
- There are three types of rule collections:
 - **Application rules:**
 - Configure fully qualified domain names (FQDNs) that can be accessed from a subnet.
 - For example, specify the Windows Update network traffic through the firewall.
 - **Network rules:**
 - Similar like NSG
 - Non-HTTP/S traffic must have a network rule to pass through the firewall.
 - If resources one subnet must communicate with another, you would configure a network rule from source to destination.
 - **DNAT rules:**
 - Destination Network Address Translation (DNAT)
 - Translate and filter inbound traffic to your subnets.
 - Translate your firewall public IP and port to a private IP and port.

Azure Firewall Features

- **High availability:** Azure Firewall does not require any additional settings or services. It is fully managed and has a very good uptime.
- **Availability zones:** Based on your needs, a firewall can be made available across various availability zones or restricted to specific zones. There is no extra charge for this, however data transfer rates may vary based on the zones.
- **Scalability:** The firewall can be scaled to meet the changing needs of the network.
- **Traffic filtering rules:** Rules for allowing or disallowing connections can be established based on IP addresses, ports, and other factors. Azure Firewall can differentiate between packets from various connections and apply rules to accept or deny them.
- **FQDN tags:** Tags for fully qualified domain names (FQDNs) can be assigned to trustworthy sources that need to pass across the firewall. Based on this, rules may be built to allow traffic from qualifying domains to pass through.
- **Service tags:** These are labels for Azure Key Vault, Container Registry, and other services that represent a range of IP addresses. These are handled by Microsoft and cannot be modified. These may be used to create filtering rules in the firewall.

Azure Firewall Features

- Threat intelligence: Microsoft maintains a threat intelligence field that contains a list of harmful sources and domains. Azure Firewall can utilize this information to block connections or notify users.
- Multiple public IP addresses: Azure Firewall allows you to add up to 250 IP addresses.
- Azure Monitor logging: Azure Monitor and Azure Firewall are tightly connected. As a result, all occurrences are logged, and these logs may be preserved or broadcast to event hubs, among other things.
- Web categories: Administrators can grant or refuse access to certain websites based on which category they fall into. This can include social networking sites, gaming sites, and other types of websites.
- Certifications: All of the following certifications are available for Azure Firewall: Payment Card Industry (PCI), Service Organization Controls (SOC), International Organization for Standardization (ISO), and ICSA Labs.

Firewall vs NSG

- | | | |
|--|--|--|
| <ul style="list-style-type: none">➤ Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network- and application-level protection across different subscriptions and virtual networks.➤ Support application FQDN tags➤ Can mask the source and destination network addresses➤ Threat Intelligence➤ Can analyze and filter L3-L7 application traffic➤ Robust and Fully managed service | | <ul style="list-style-type: none">➤ Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription.➤ Missing➤ Missing➤ Missing➤ Missing➤ Basic firewall |
|--|--|--|

Azure Load Balancer

Deliver high availability and network performance to your apps

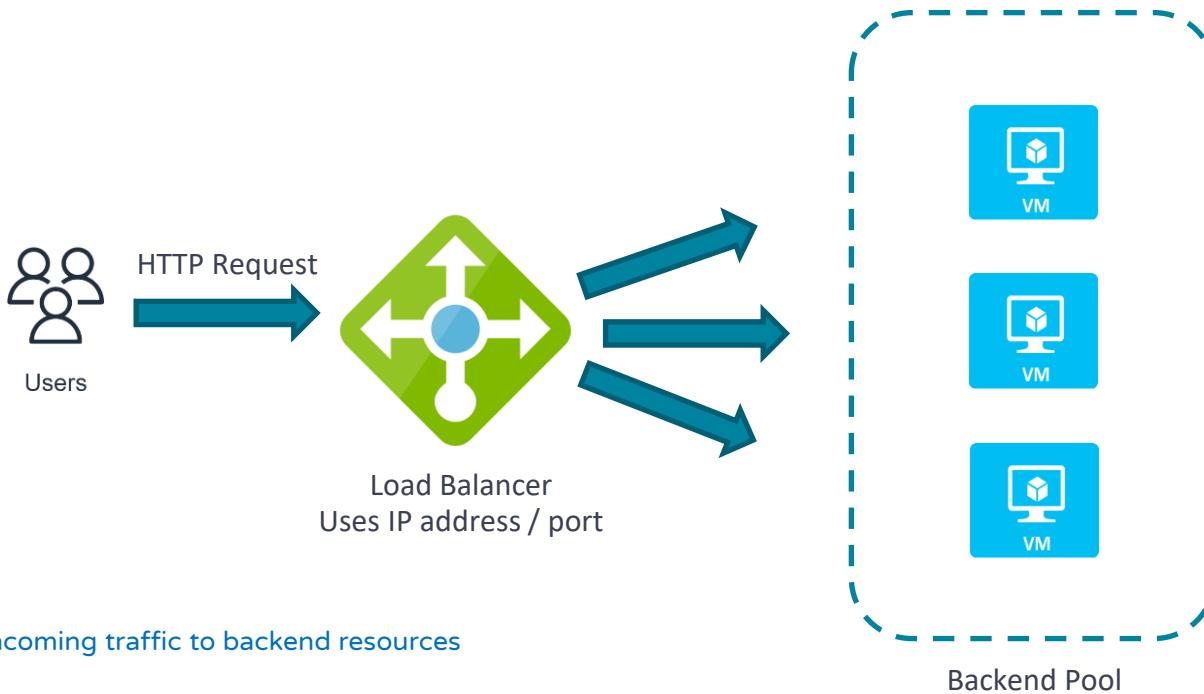
Load Balancer



Users



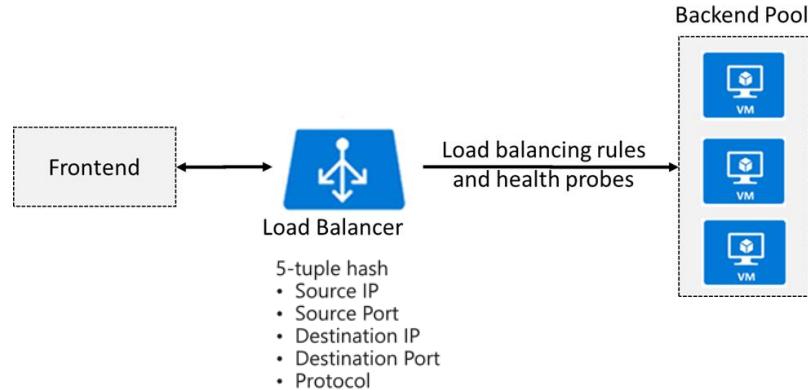
Load Balancer



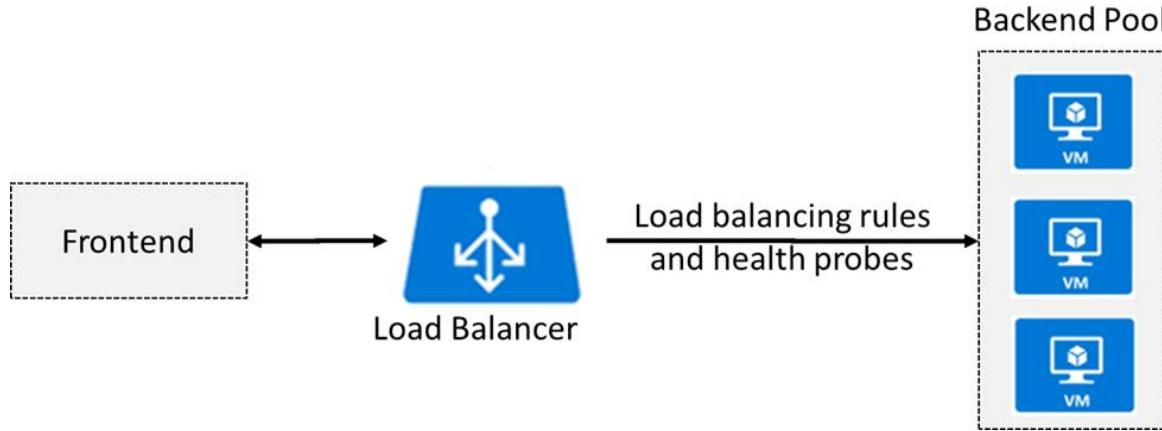
- Distribute incoming traffic to backend resources
- Provides:
 - High Availability
 - Scalable performance

Load Balancer Components

- Frontend configuration – IP address of your Azure Load Balancer. It's the point of contact for clients.
- Backend pool – Group of virtual machines that is serving incoming traffic.
 - Adding or removing VMs from the backend pool reconfigures the load balancer without additional operations.
- Load-balancing rules determine how traffic is distributed to the backend pool.
- Health probes ensure the resources in the backend are healthy.
 - Health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks.
 - When a probe fails to respond, the load balancer stops sending new connections to the unhealthy instances.

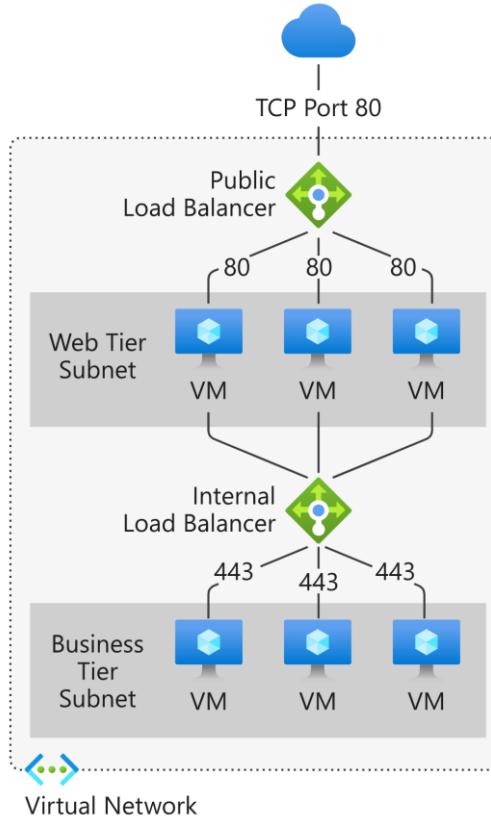


Demo: Basic Load Balancer Implementation



Load Balancer - Public vs Internal

- Two types of load balancers: Public and Internal
- A public load balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM.
- An internal load balancer directs traffic to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.

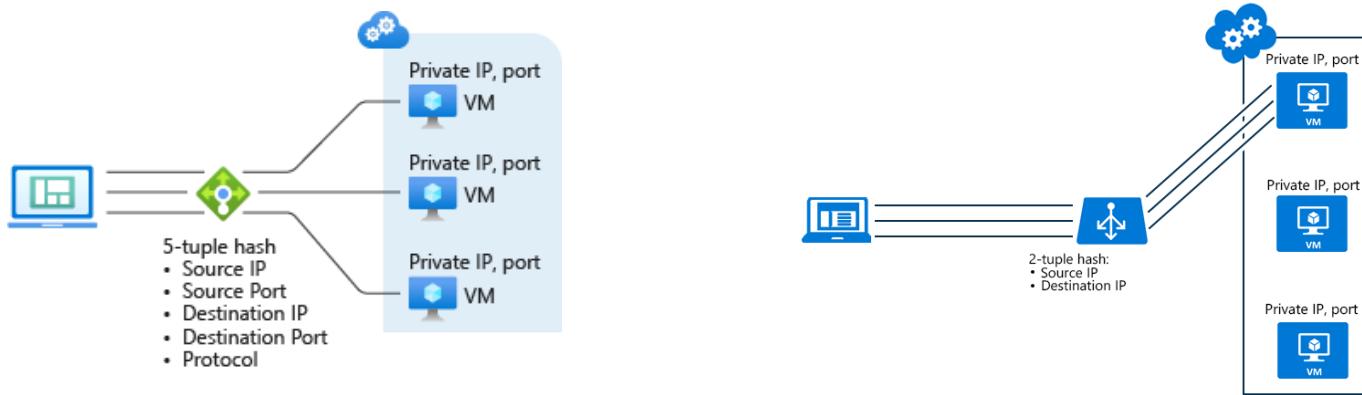


Load balancer SKUs (stock keeping unit)

	Basic	Standard
Cost	Free	Cost per hour
Backend pool Size	Supports up to 300 instances	Support up to 1000 instances
Backend pool endpoints	Only VMs in single availability set or scale set	Any VM in single Vnet.
VM Public IP type	Basic SKU Public IP or No Public IP	Standard SKU Public IP or No Public IP
NSG Rules	Open by default. Network security group optional.	Closed to inbound flows unless allowed by a network security group.
Health Probe	TCP, HTTP	TCP, HTTP, HTTPS
Availability Zones	No Support	Support
SLA	Not available	99.99%
Use Azure LB SKU can't be changed after creation (not mutable)	Dev/Test	Production

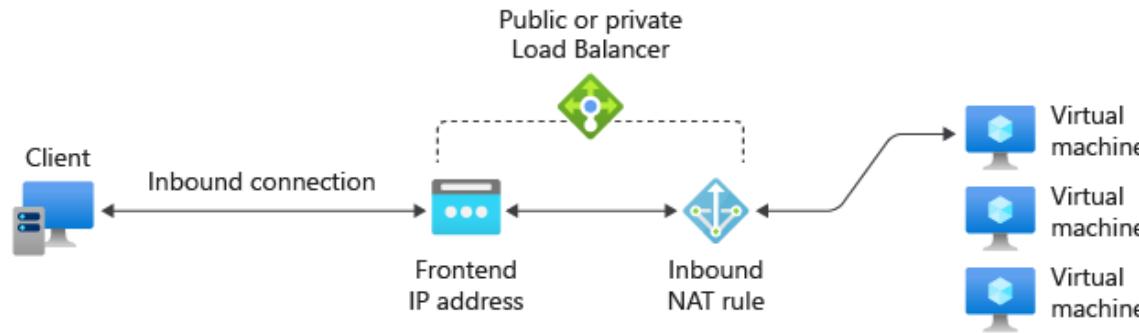
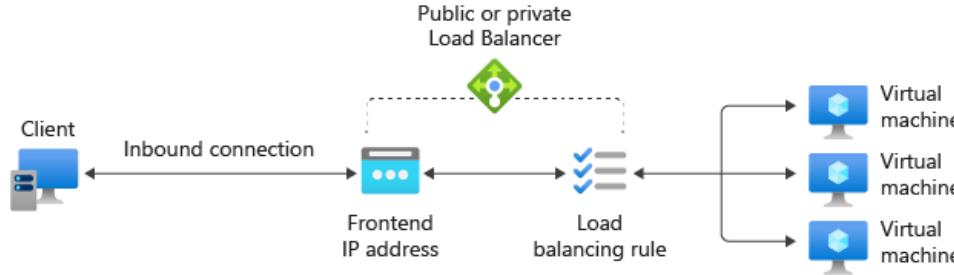


Load Balancer distribution modes



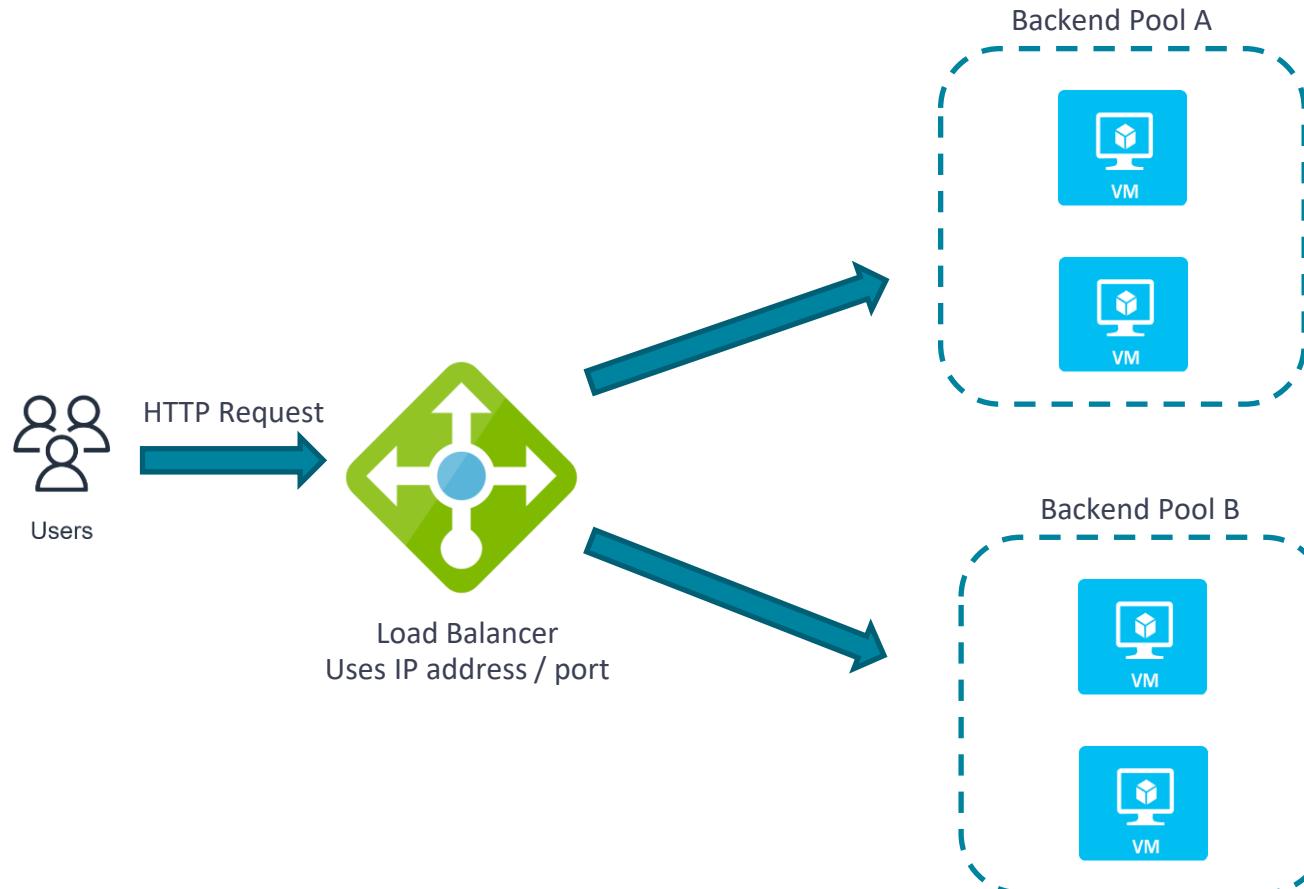
Distribution mode	Hash based	Session persistence: Client IP	Session persistence: Client IP and protocol
Overview	Traffic from the same client IP is routed to any healthy instance in the backend pool	Traffic from the same client IP is routed to the same backend instance	Traffic from the same client IP and protocol is routed to the same backend instance
Tuples	5 tuple	2 tuple	3 tuple
Azure portal configuration	Session persistence: None	Session persistence: Client IP	Session persistence: Client IP and protocol

Demo: Load Balancer- NAT Rules

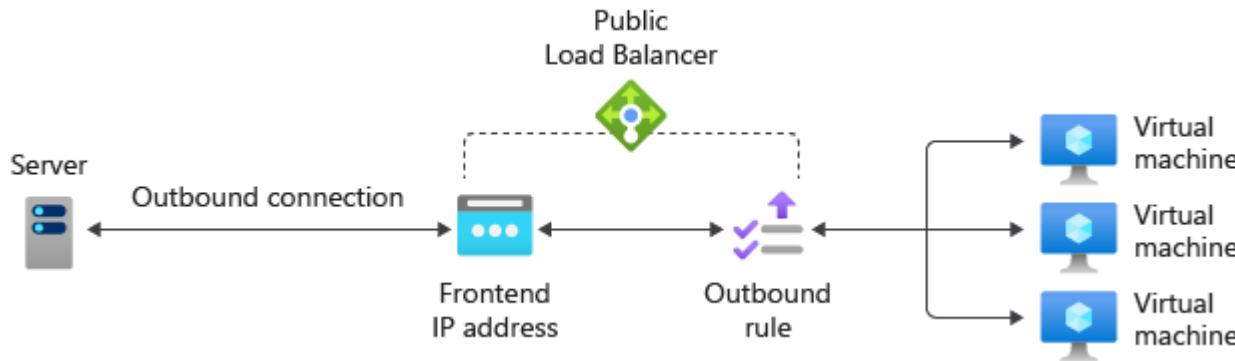


- An inbound NAT rule forwards incoming traffic sent to frontend IP address and port combination.
- The traffic is sent to a specific virtual machine or instance in the backend pool.

Load Balancer



Load Balancer - Outbound rule



Application Gateway

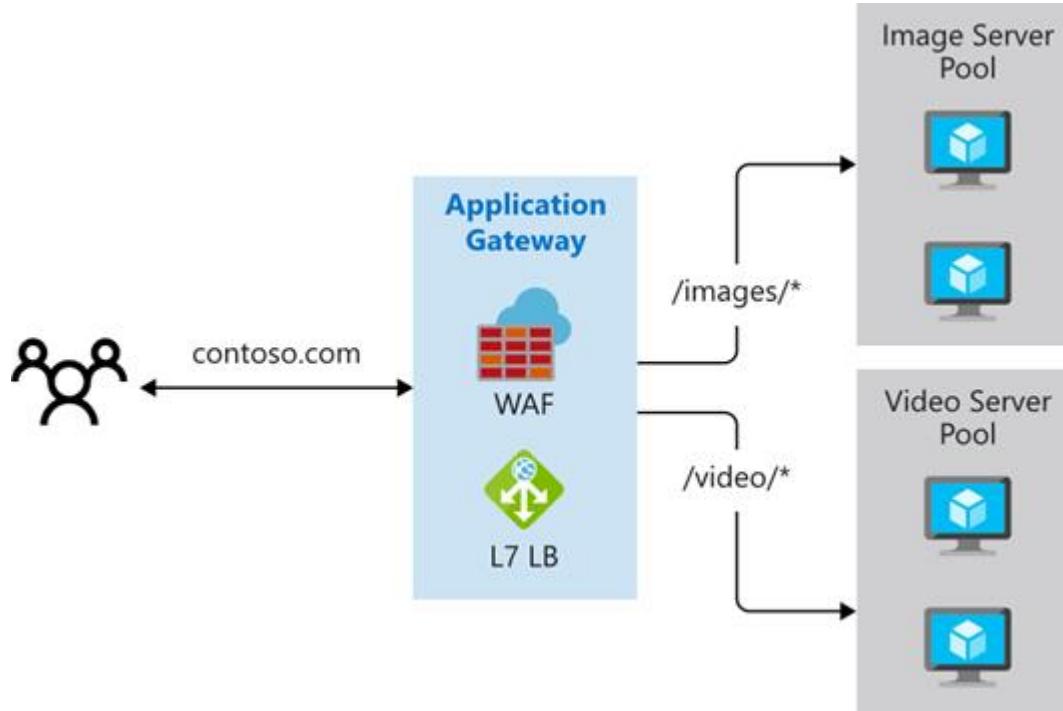
Provides HTTP based load balancing.

Application Gateway

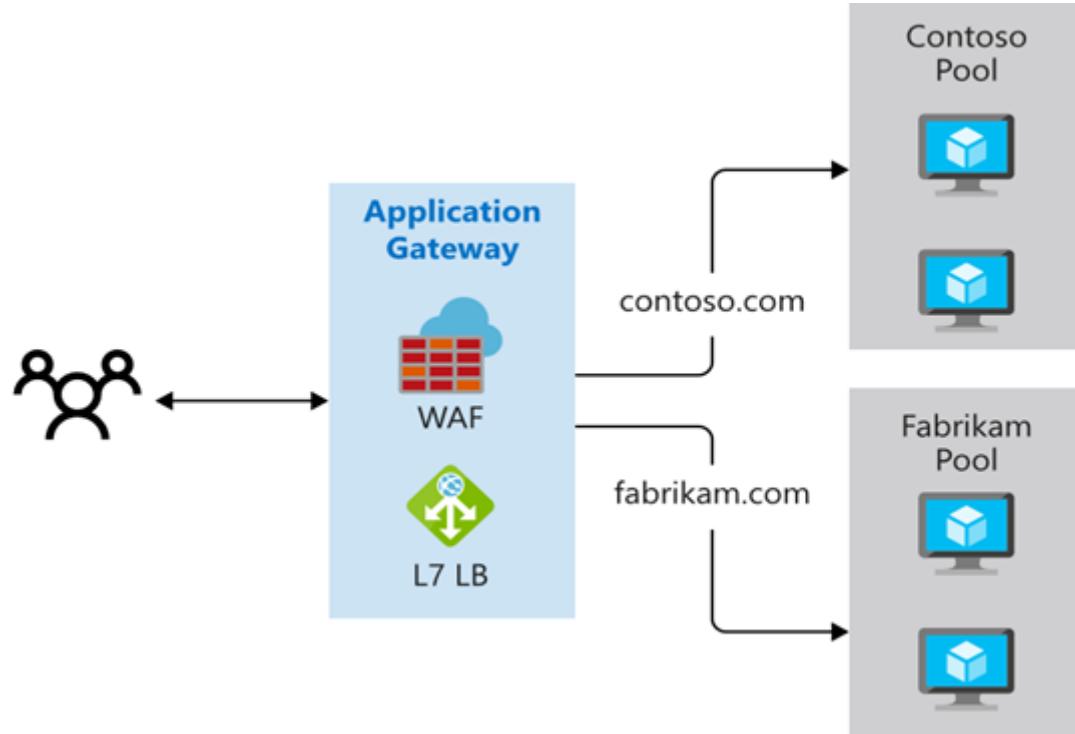
- Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.
- OSI layer-7 (Application layer) load balancer.
 - HTTP and HTTPS traffic only
 - Traditional Load Balancer → Layer 4 – TCP and UDP (source/destination IP/port and protocol)
- Routing rules based on HTTP request parameters:
 - URL path (web address)
 - Host headers (request data)
- Can be configured public facing, internal or combination of both.
- You can only assign Static IP address to application gateway.
- Needs a separate empty subnet to install application gateway components



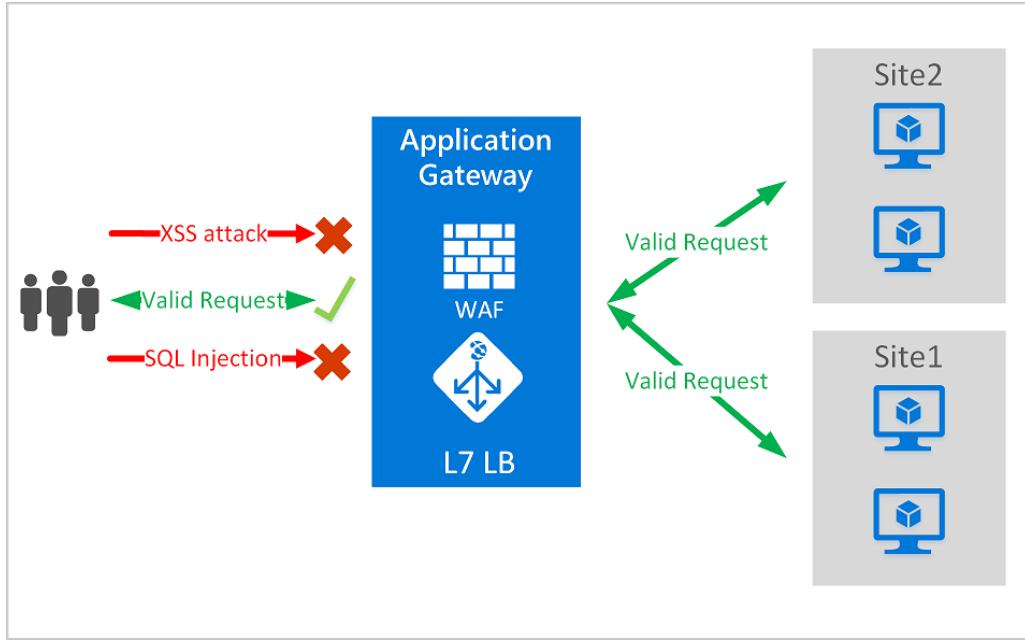
URL Path-based routing



Multiple site routing

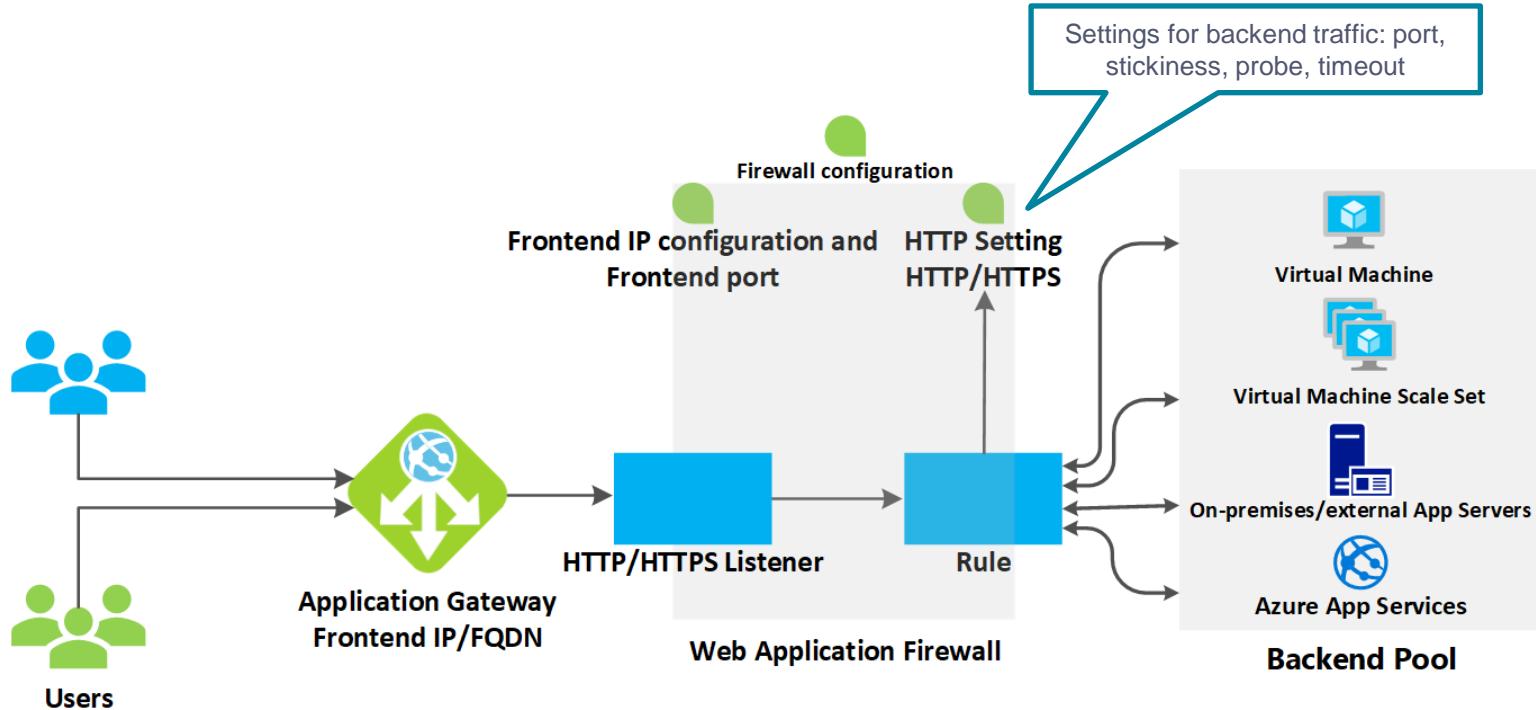


Web application firewall

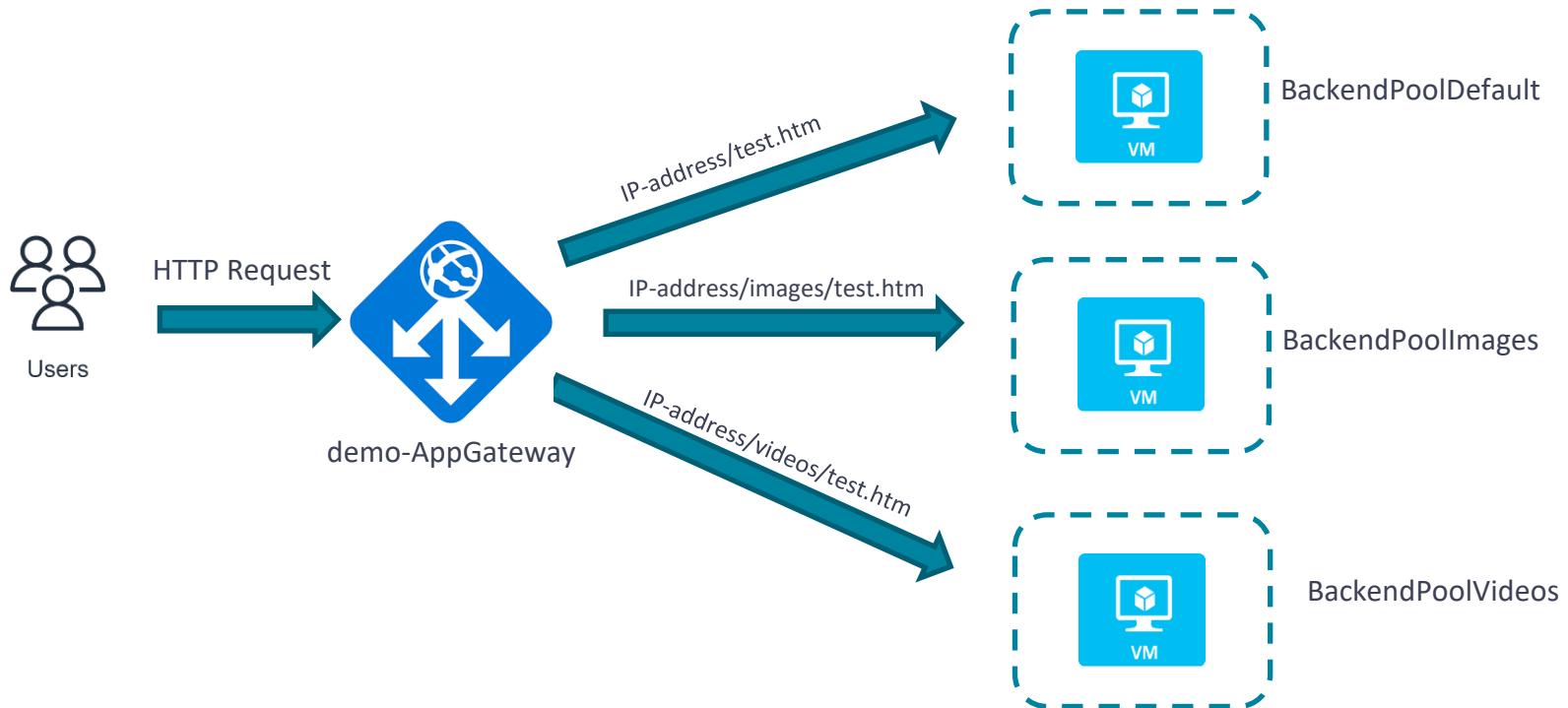


- Web application firewall
 - Checks each request for many common threats
 - Based on the Open Web Application Security Project (OWASP)
 - SQL-injection, Cross-site scripting, Command injection, HTTP request smuggling, HTTP response splitting, Remote file inclusion, Bots, crawlers, and scanners, and HTTP protocol violations and anomalies.

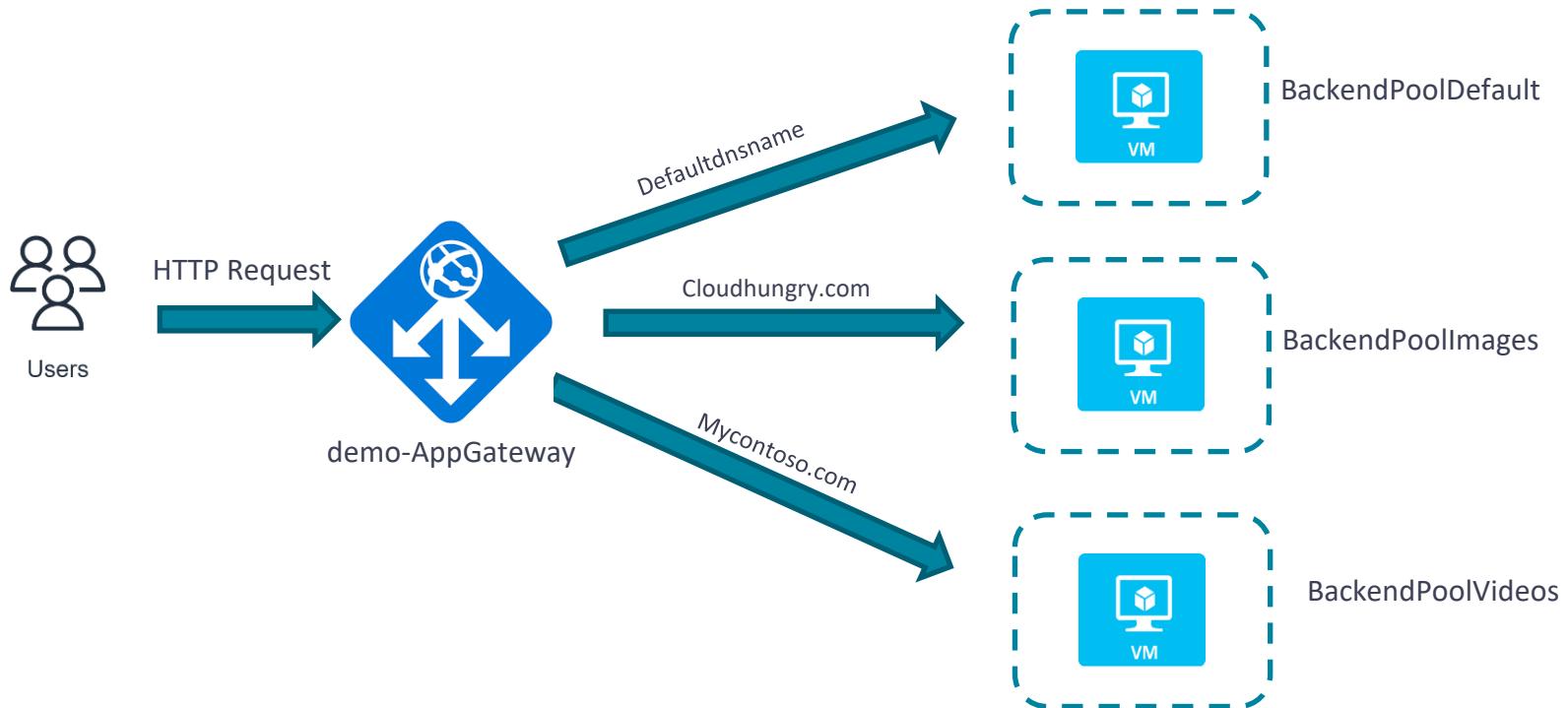
Application Gateway Components



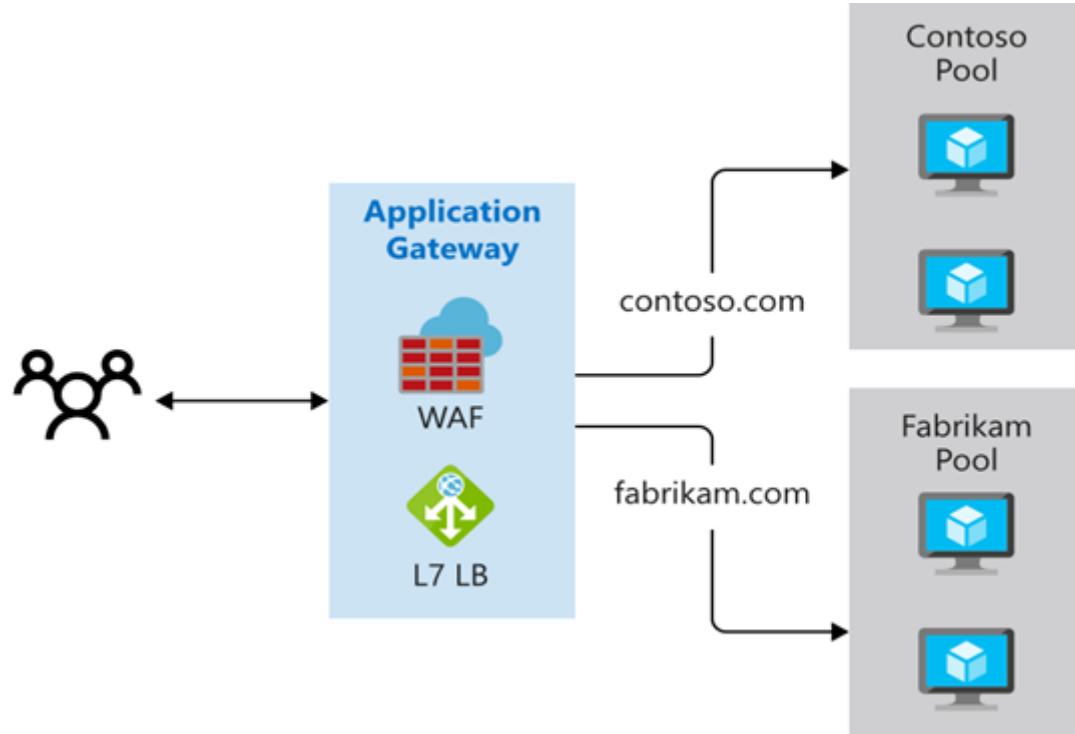
Demo: URL Path-based routing



Demo: Multiple site routing



Multiple site routing



Application Gateway Features

- Round robin load balancing
- Cookie-based session affinity: Session stickiness ensures client requests in the same session are routed to the same back-end server.
 - Session stickiness is critical for e-commerce apps, since you don't want a transaction disturbed by a load balancer.
- Web application firewall
 - Checks each request for many common threats
 - Based on the Open Web Application Security Project (OWASP)
 - SQL-injection, Cross-site scripting, Command injection, HTTP request smuggling, HTTP response splitting, Remote file inclusion, Bots, crawlers, and scanners, and HTTP protocol violations and anomalies.
- Application Gateway routing
 - Path-based routing
 - Multiple-site routing
- Support Secure Socket Layer (SSL/TLS termination)
 - Thus communication to backend servers is unencrypted.
 - This functionality reduces web server encryption and decryption burden/costs.

Application Gateway Features

- **Redirection:** Redirection can be used to another site, or from HTTP to HTTPS.
- **Rewrite HTTP headers:** Rewriting these HTTP headers helps you add security-related header fields or Removing response header fields that can reveal sensitive information.
- **Custom error pages:** Application Gateway allows you to create custom error pages instead of displaying default error pages. You can use your own branding and layout using a custom error page.
- **Autoscaling:** can scale up or down based on changing traffic load patterns. Autoscaling also removes the requirement to choose a deployment size or instance count during provisioning.
- **Connection draining:** Connection draining helps you achieve graceful removal of backend pool members during planned service updates. Once enabled, Application Gateway ensures all deregistering instances of a backend pool don't receive any new request while allowing existing requests to complete within a configured time limit.
- **Support Websocket and HTTP/2 traffic:** There's no user-configurable setting to selectively enable or disable WebSocket support.
- **Zone redundancy:** A Standard_v2 Application Gateway can extent multiple Availability Zones, offering better fault resiliency and removing the need to provision separate Application Gateways in each zone.

Application Gateway vs Load Balancer

Azure Application Gateway

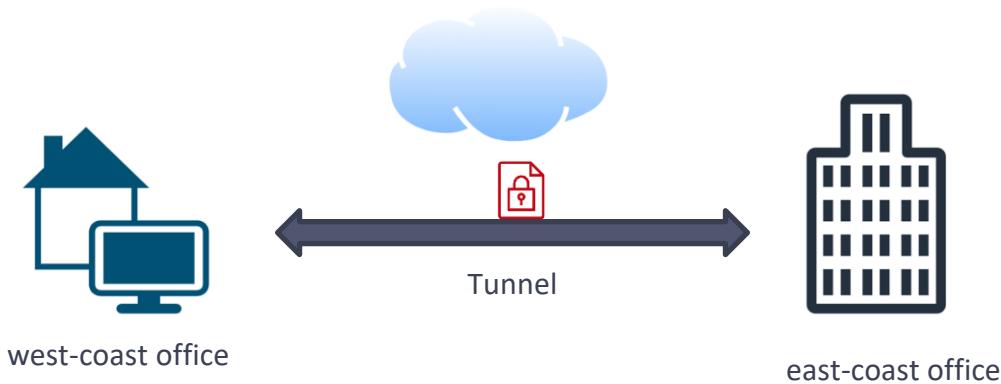
- OSI Layer 7 (Application Layer)
- HTTP/HTTPS and WebSockets
- Load Balancing – Round Robin or based on URL (path or domain name)
- Deployed in Vnet within reserved subnet
- Web Application Firewall (WAF)
- SSL/TLS offload

Azure Load Balancer

- OSI Layer 4 (Transport Layer)
- Any (TCP/UDP) workload
- Load Balancing mode – 5 tuple
- No such requirement
- Missing
- Missing

VNet connectivity

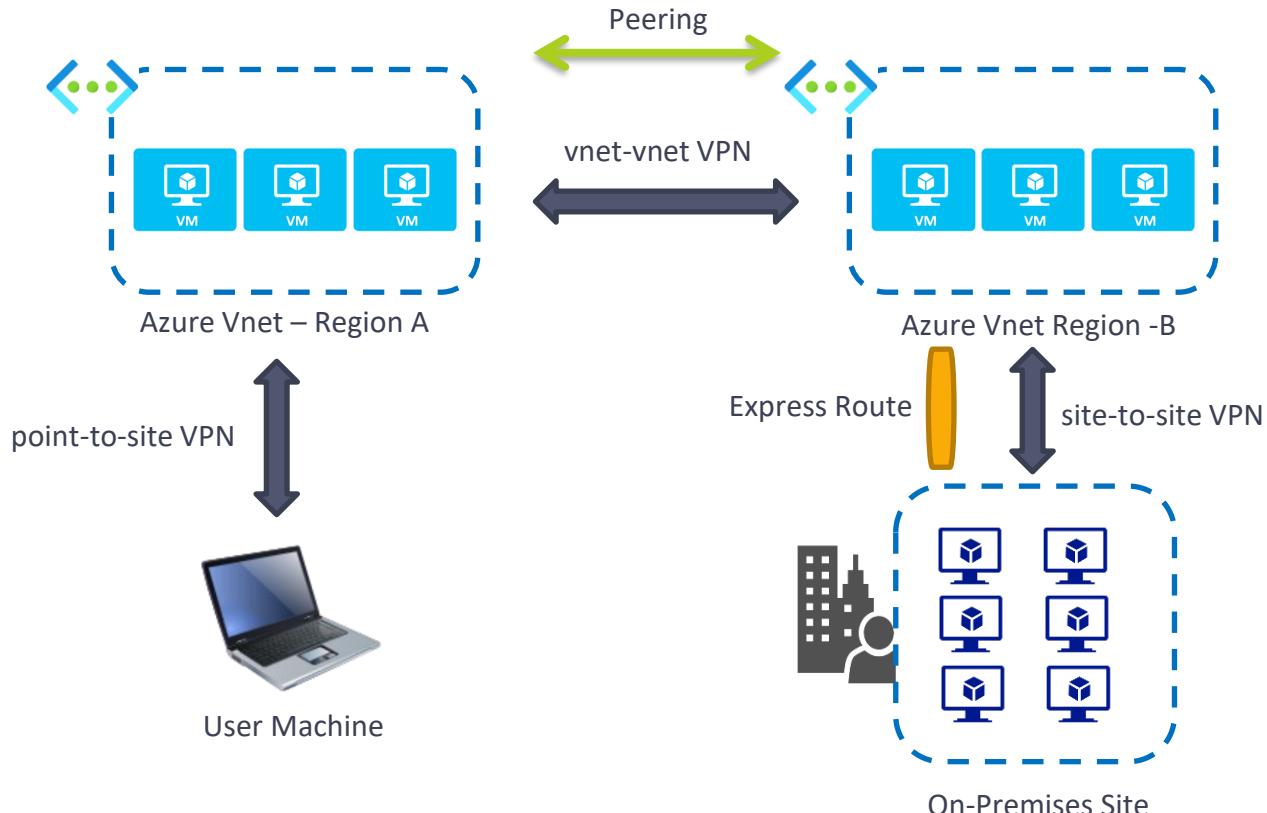
VPN (Virtual private network)



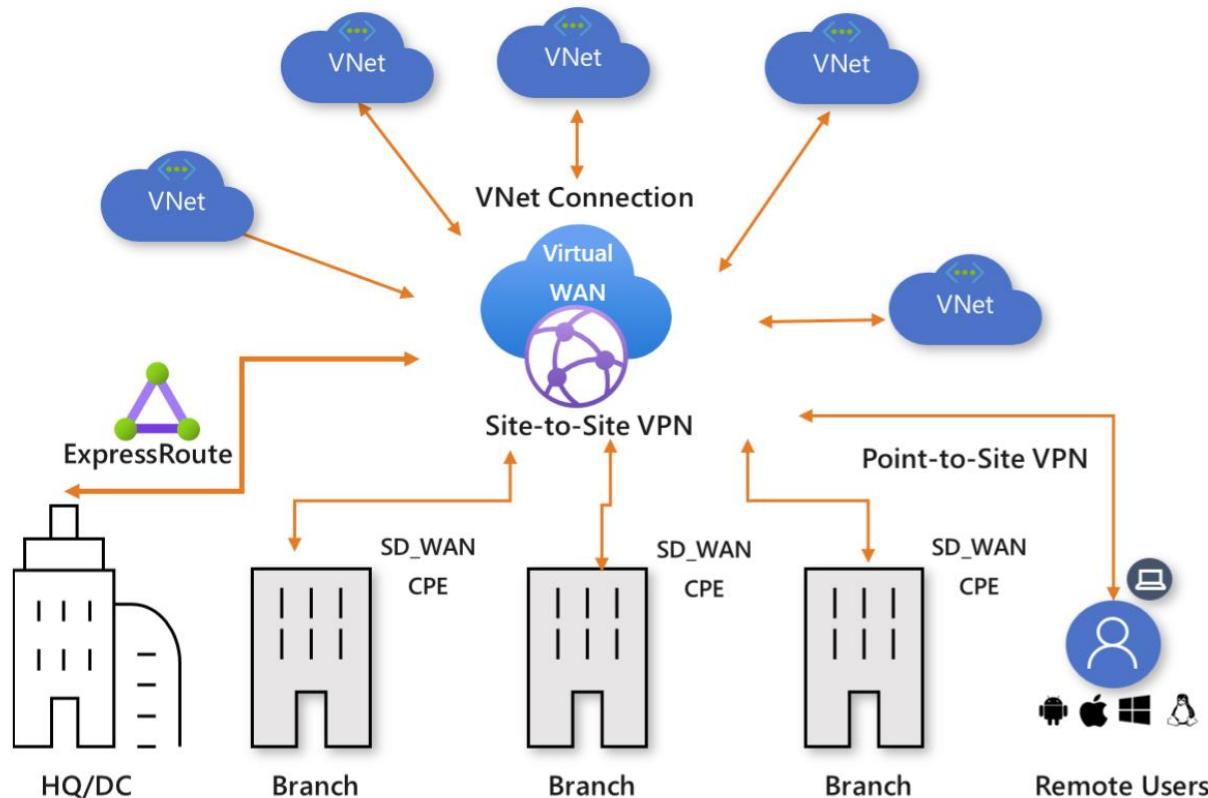
- A secure, encrypted connection over an unsecure/untrusted network (public internet)
- Traffic is encrypted while traveling over the untrusted network to prevent attacks.

Virtual Network connectivity

- VPN Connections
 - Over Internet
 - Use tunnel
 - Encrypted, secure
 - Slow
- Peering
 - Use Microsoft backbone
 - High bandwidth connection
 - low latency
 - Secure
- Express Route
 - Private Wired Connection
 - Secure
 - Complex
 - Only for Large organizations or mission critical workload



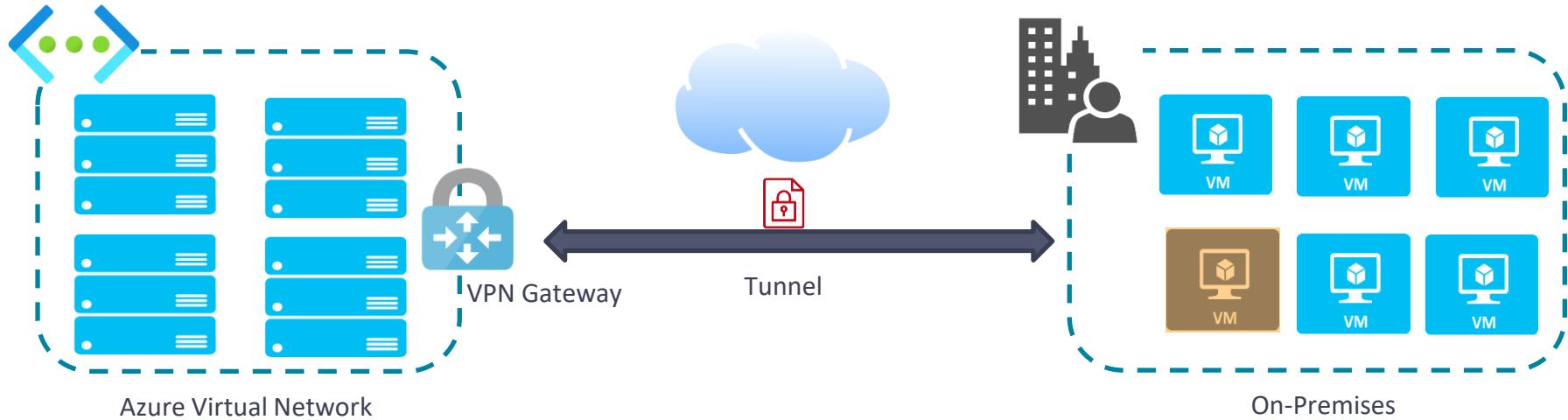
Virtual WAN



VPN Gateway

Connecting your infrastructure to the cloud

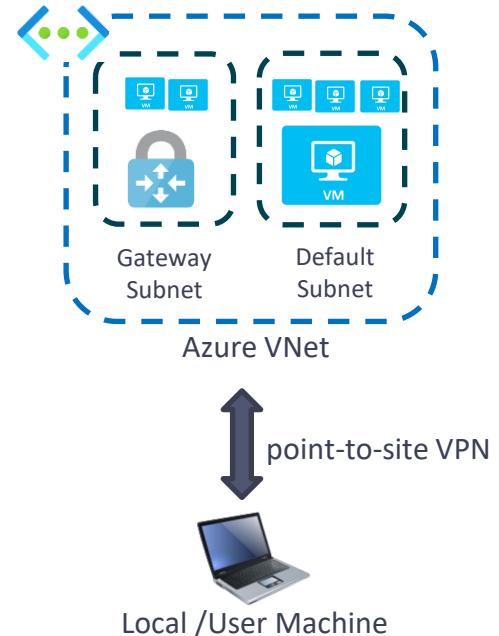
Virtual Network Gateway



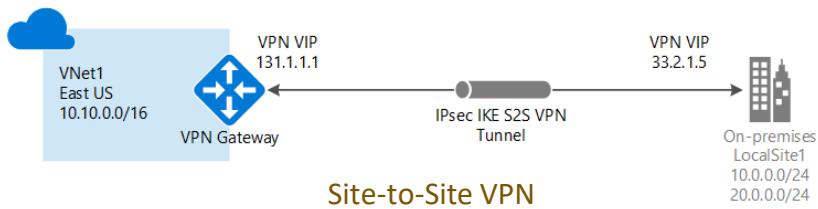
- There are two types of Virtual Network Gateway
 - VPN Gateway
 - ExpressRoute
- VPN Gateway sends encrypted traffic between an Azure VNet and an on-premises location over the public Internet.
 - Can also use to connect diff VNets using encrypted tunnel.
- Each virtual network can have only one VPN gateway.
 - However, you can create multiple connections to the same VPN gateway.

VPN Gateway

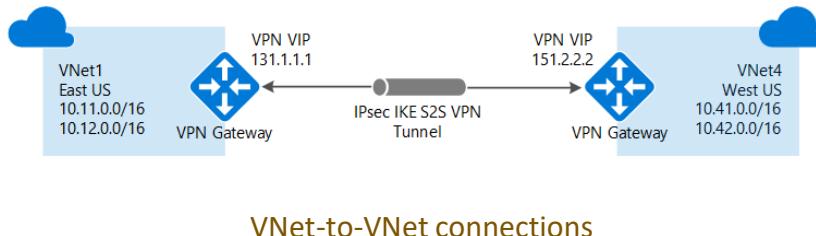
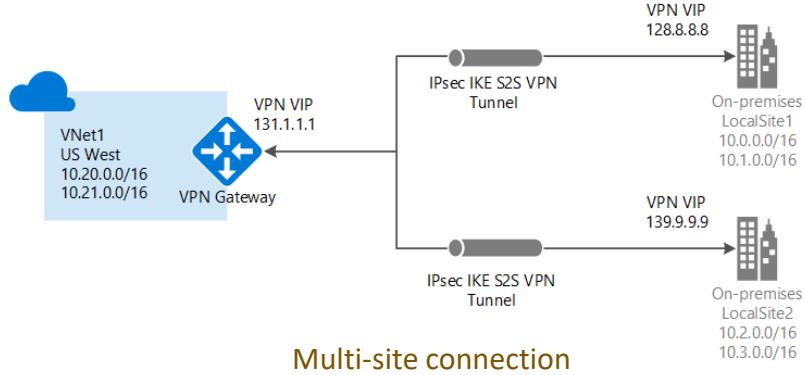
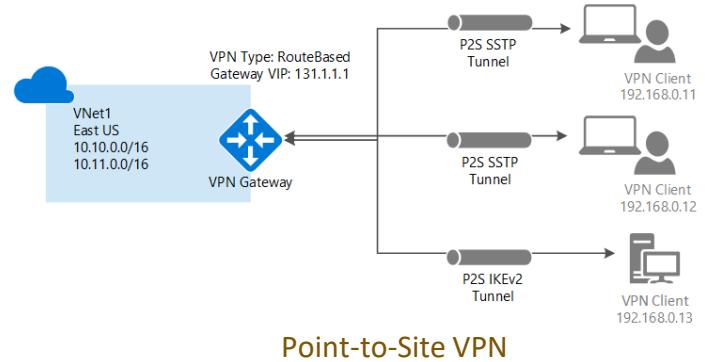
- How it works?
 - We have to deploy “Gateway subnet”
 - A virtual network gateway consists of two or more VMs automatically configured and deployed to the gateway subnet.
 - The gateway VMs contain routing tables and run specific gateway services.
 - This behind the scene infrastructure managed automatically by Azure and do not require administrative attention.
- Gateway SKUs : number of tunnels, max bandwidth, throughputs, features, and SLAs
- Pricing: Hourly compute cost + egress data transfer
- Types of Azure VPN Gateway you can choose from:
 - Policy based - Static routing
 - Only 1 tunnel
 - Only S2S connection
 - Support for IKEv1 only
 - Generally use for compatibility with legacy on-premises VPN devices
 - Route based - Dynamic routing
 - Multiple tunnels
 - Supports IKEv2



VPN Gateway design



VPN Client Address Pool: 192.168.0.0/24



VPN gateway - High Availability

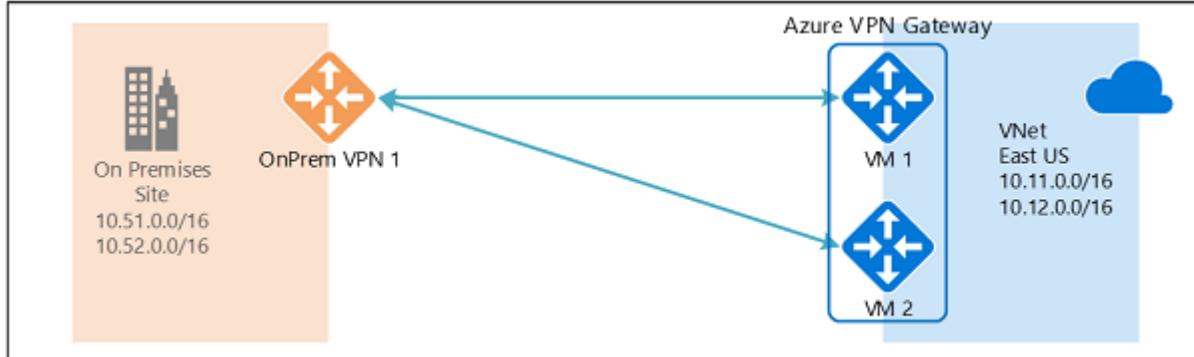
Active/standby

- Azure VPN gateway consists of two instances
- For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the connections.
- switch over will cause a brief interruption



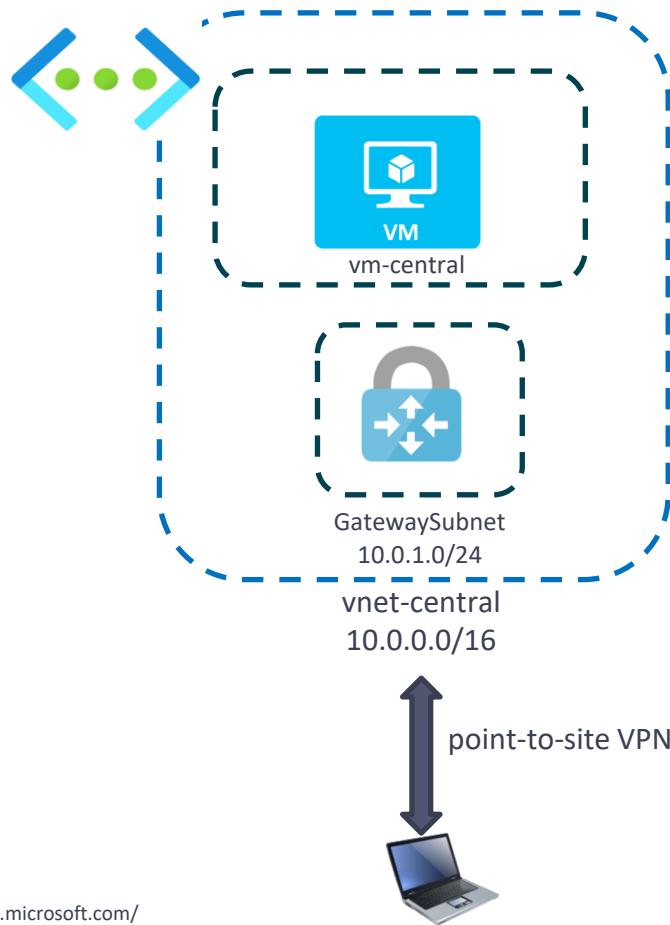
Active/active

- Both instances of the gateway VMs will be active and establish connection.
- If planned maintenance or unplanned event happens to one gateway instance, the traffic will be switched over to the other active tunnel automatically.

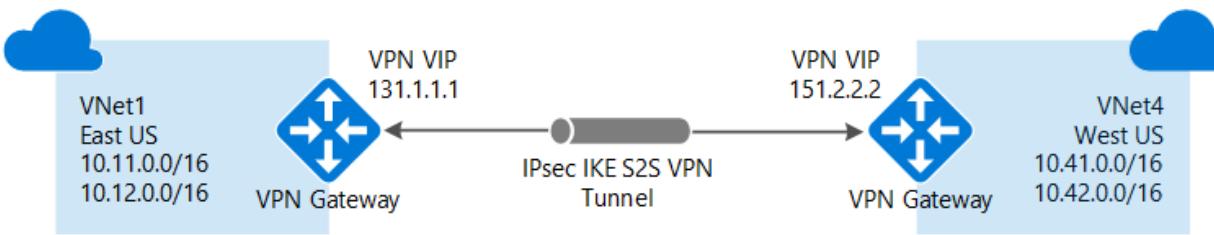


Point-to-site VPN connection

- Use to connect a single computer to an Azure virtual network.
- Commonly used by remote workers with portable computers.

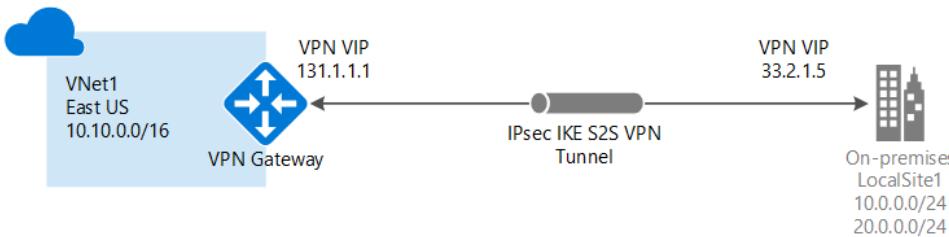


VNet-to-VNet VPN Connection



- Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE
- VNets can be in the:
 - Same or different regions
 - Same or different subscriptions (have to use powershell or CLI)
- Local Network gateways are automatically created and populated
- If you update the address space for one VNet, the other VNet automatically knows to route to the updated address space
- VNet-to-VNet traffic within the same region is free for both directions
- Cross region VNet-to-VNet egress traffic is charged with the outbound inter-VNet data transfer rates

Site-to-Site (S2S) VPN connection



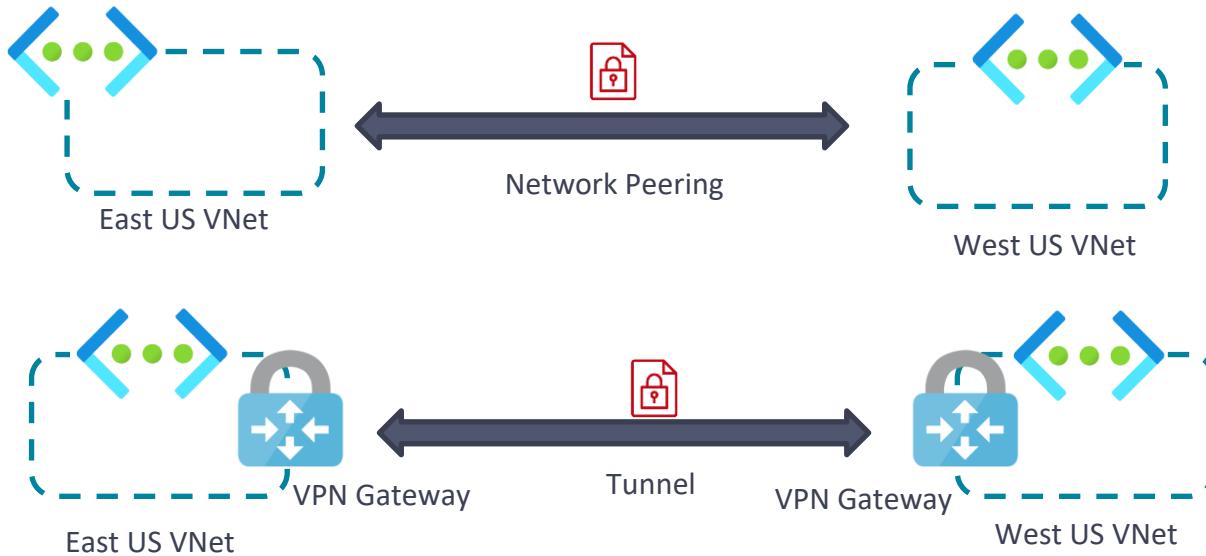
- Allows you to connect one network to another network with traffic between the two networks passing across an encrypted VPN tunnel.
- Used to connect:
 - On-premises sites to Azure VNet
 - Azure VNet to VNet
- Protocols: Internet protocol security (IPSec), internet key exchange (IKE, IKEv2)
- Scenarios
 - Capacity on-demand: Your on-premises datacenter may be expanded without new equipment.
 - Migration: migrate resources/data to Azure
 - Disaster recovery
- There should not be duplicate address range between two networks
- Multi-Site VPN Connection: More than one networks connect with VPN Gateway

VNet Peering

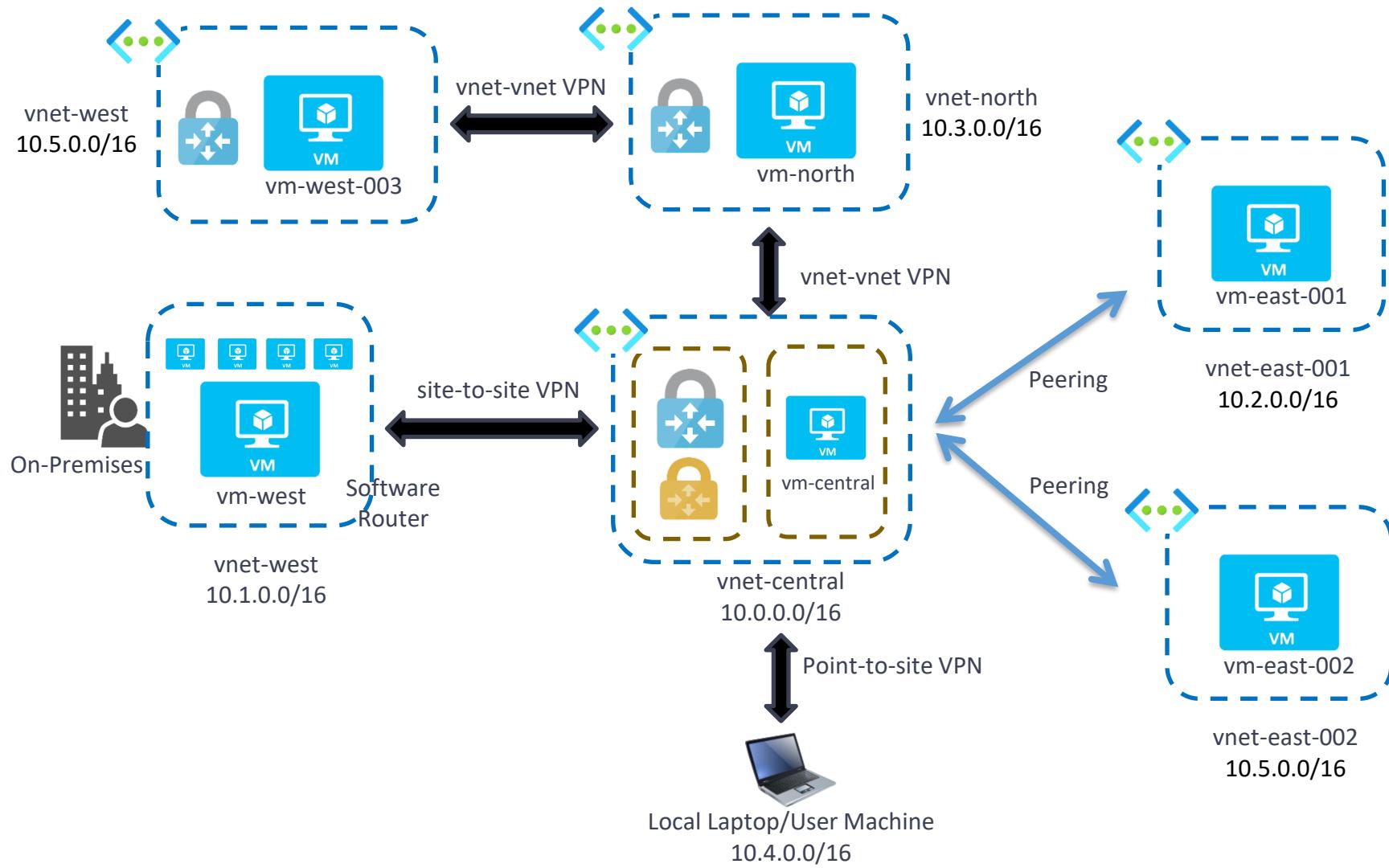


- Connect two Azure VNet
- Traffic route through the Microsoft backbone infrastructure
- Azure supports:
 - VNet peering: same Azure region
 - Global VNet peering: across different Azure regions
- Benefits:
 - Low latency, high bandwidth connection
 - Secure because using Azure internal networks (not internet like VPN)
 - Can transfer data across Azure subscription and regions
 - Faster and easier to setup
 - No public IP required
- Cannot use overlapping address range
- Peering relationship is not transitive.

VPN Gateway vs Vnet Peering

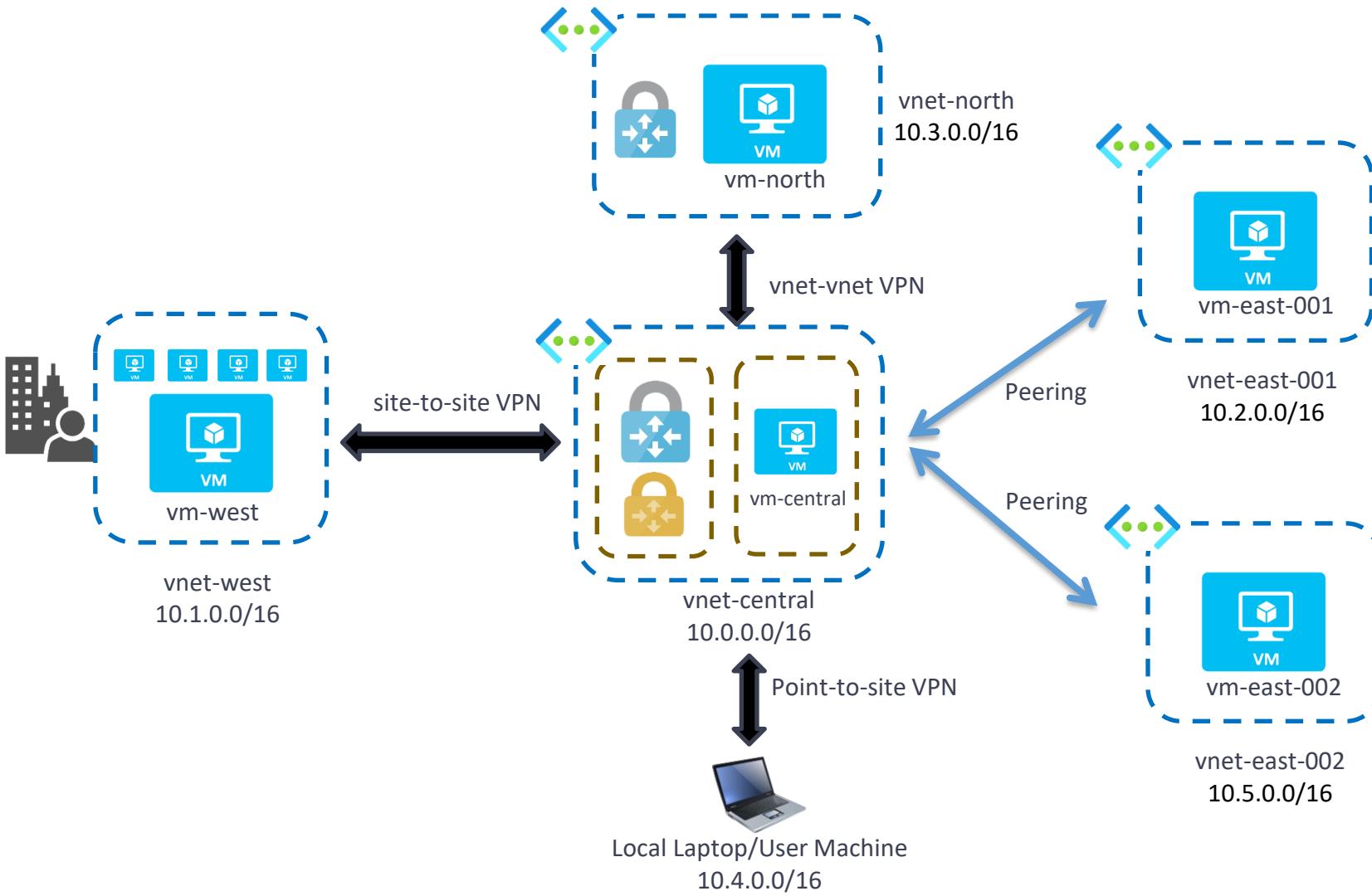


- Which is best for you?
 - **VNet Peering** provides a low latency, high bandwidth connection useful in scenarios such as cross-region data replication and database failover scenarios. Since traffic is completely private and remains on the Microsoft backbone, customers with strict data policies prefer to use VNet Peering as public internet is not involved. Since there is no gateway in the path, there are no extra hops, ensuring low latency connections.
 - **VPN Gateways** provide a limited bandwidth connection and is useful in scenarios where encryption is needed, but bandwidth restrictions are tolerable. In these scenarios, customers are also not as latency-sensitive.

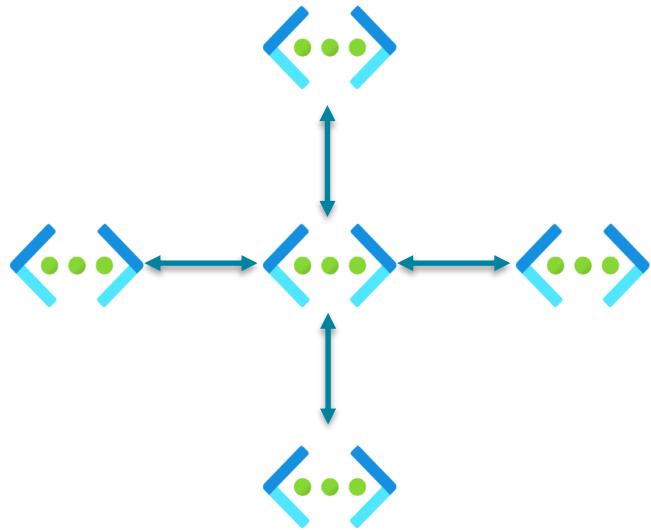


Azure Virtual WAN

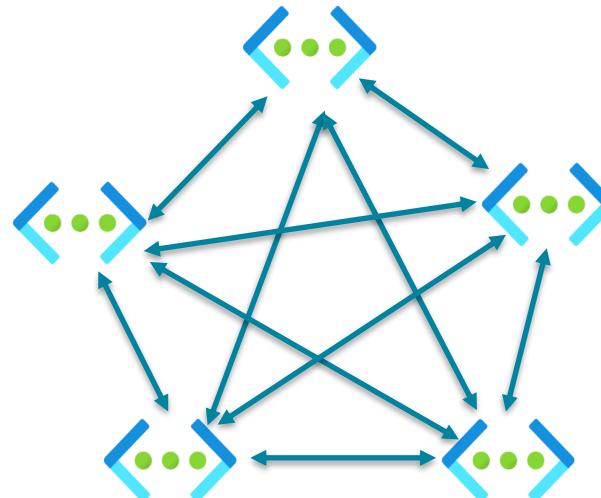
Simple, unified, global connectivity and security



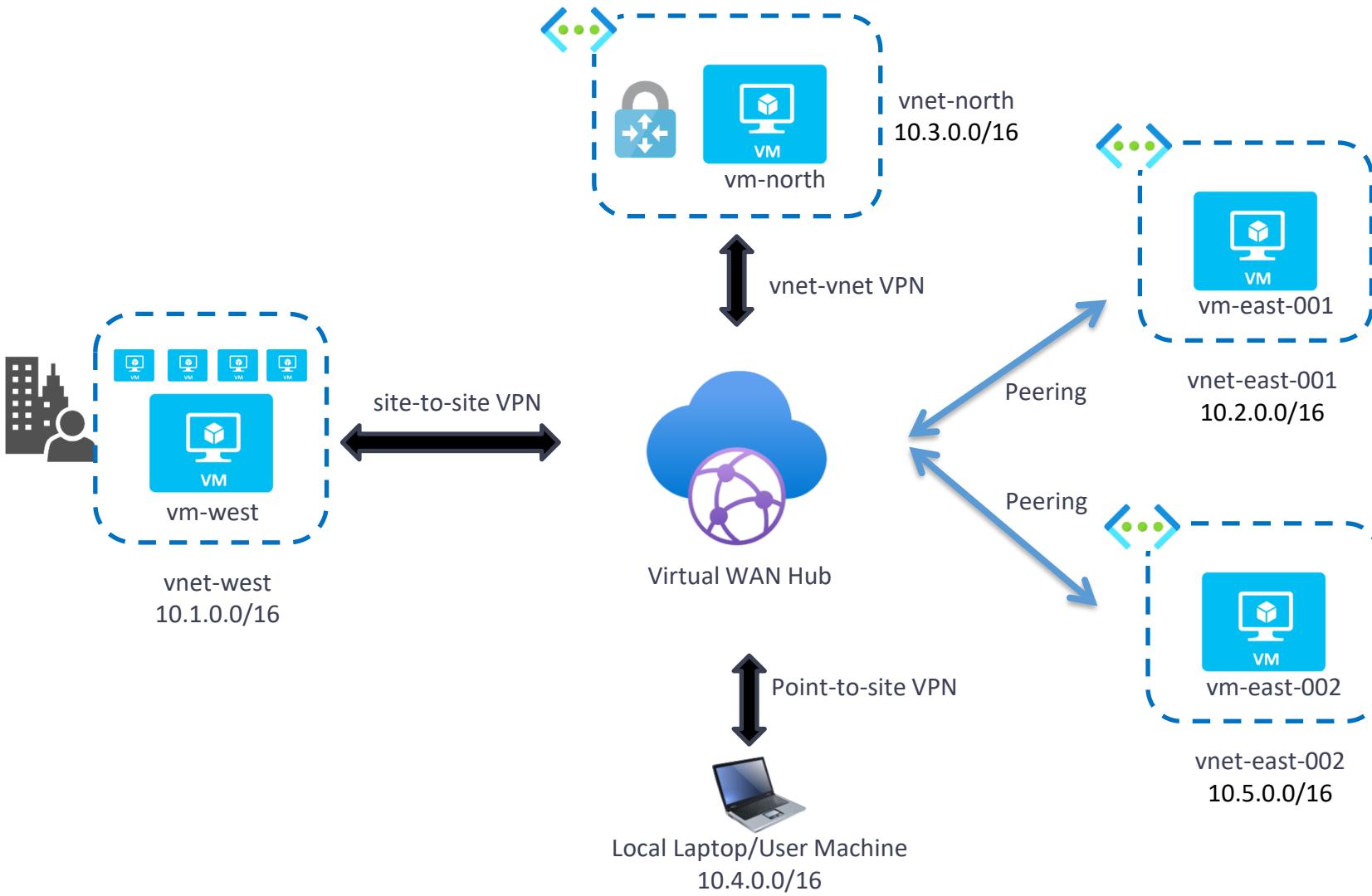
Hub-Spoke vs Mesh



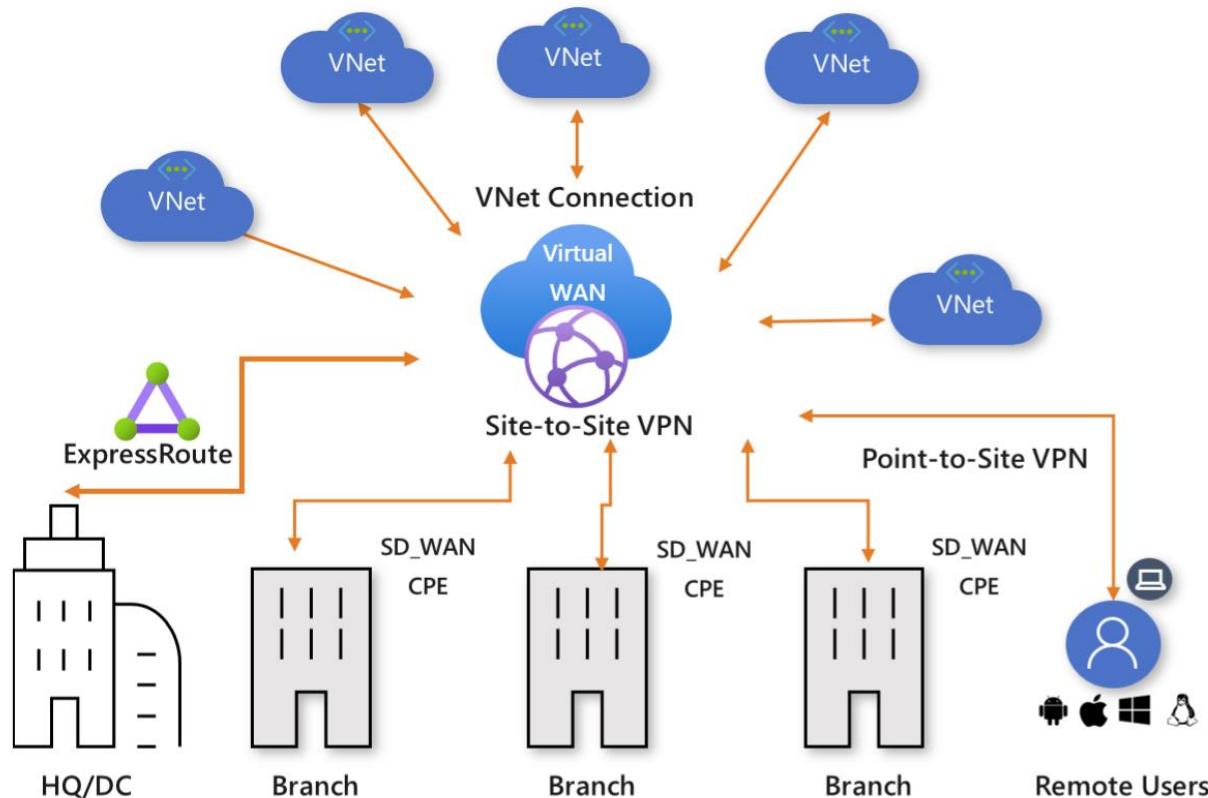
Hub-Spoke Topology



Mesh Topology

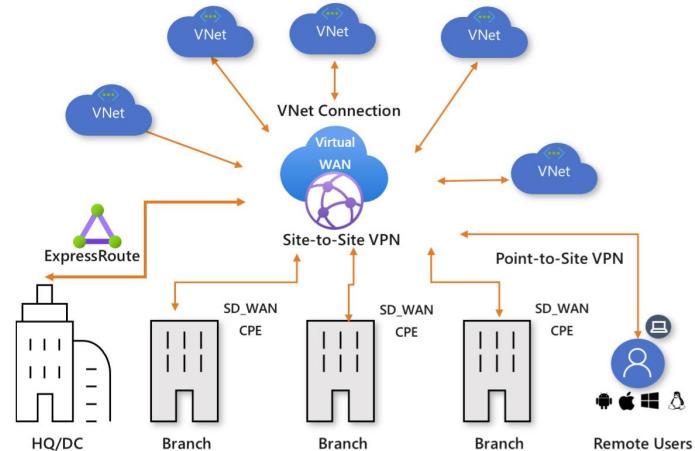


Virtual WAN

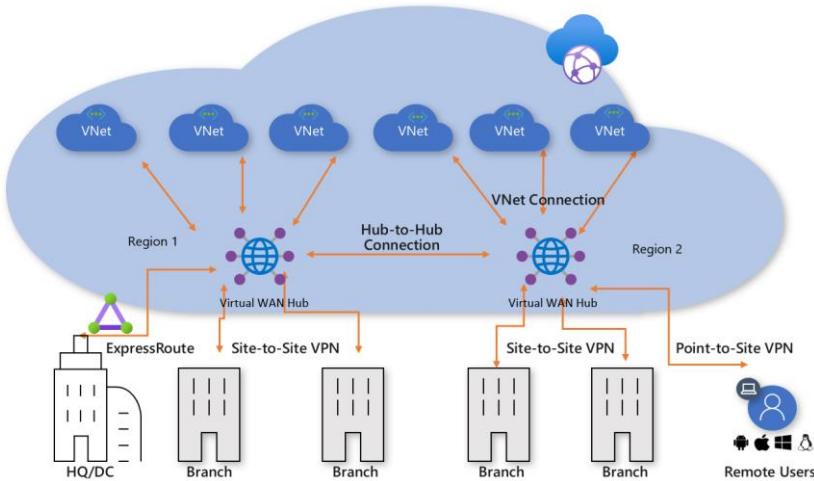


Virtual WAN

- WAN stands for “wide area network”
- Azure Virtual WAN -> software-defined WAN sometimes called SD-WAN.
- Microsoft-managed, transitive, VNet hub-and-spoke architecture.
- Virtual WAN like an umbrella which includes lots of services:
 - VNet peering
 - All Azure VPN types - point-to-site, site-to-site, vnet-to-vnet VPN connections
 - Azure ExpressRoute
 - Azure Firewall
 - Connectivity, security, monitoring and routing features like user-defined routing (UDRs), and route tables..
- With Virtual WAN you have a single management interface for these services.

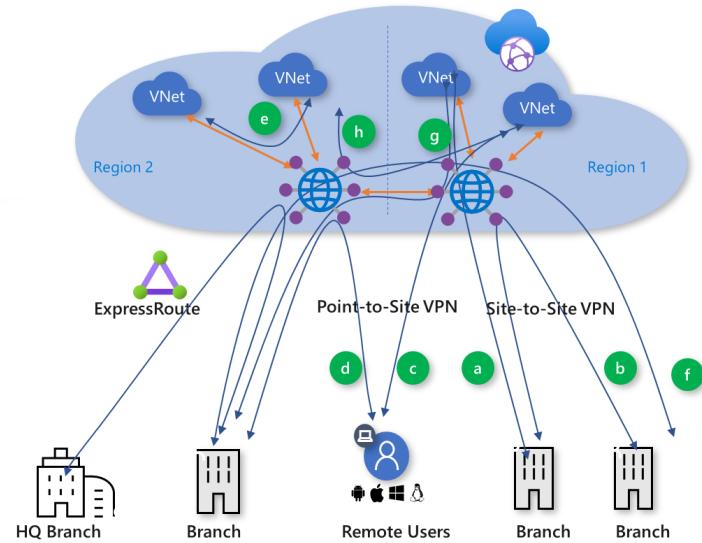
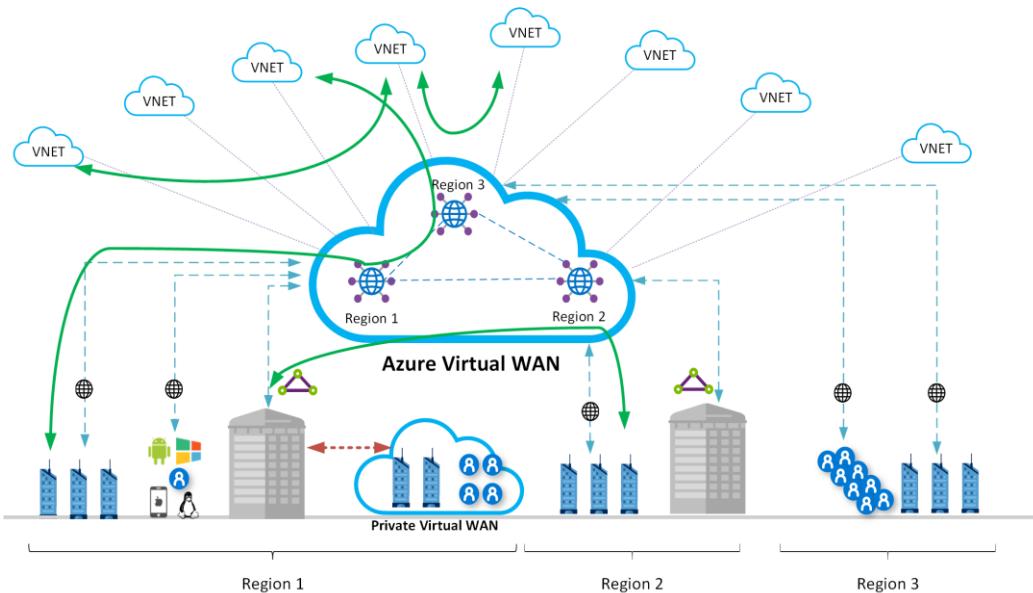


Virtual WAN global transit



- Global transit network architecture will connect cloud and on-premises network endpoints across regions.
- Hubs are automatically interconnected via hub-to-hub links
- Using Azure Global Network's hub-to-hub connection, traffic from a cloud-connected branch in one region can reach another branch or VNet in a different region.
- Customers can transit traffic globally through the Microsoft Backbone without using AT&T, British Telecom, or others.

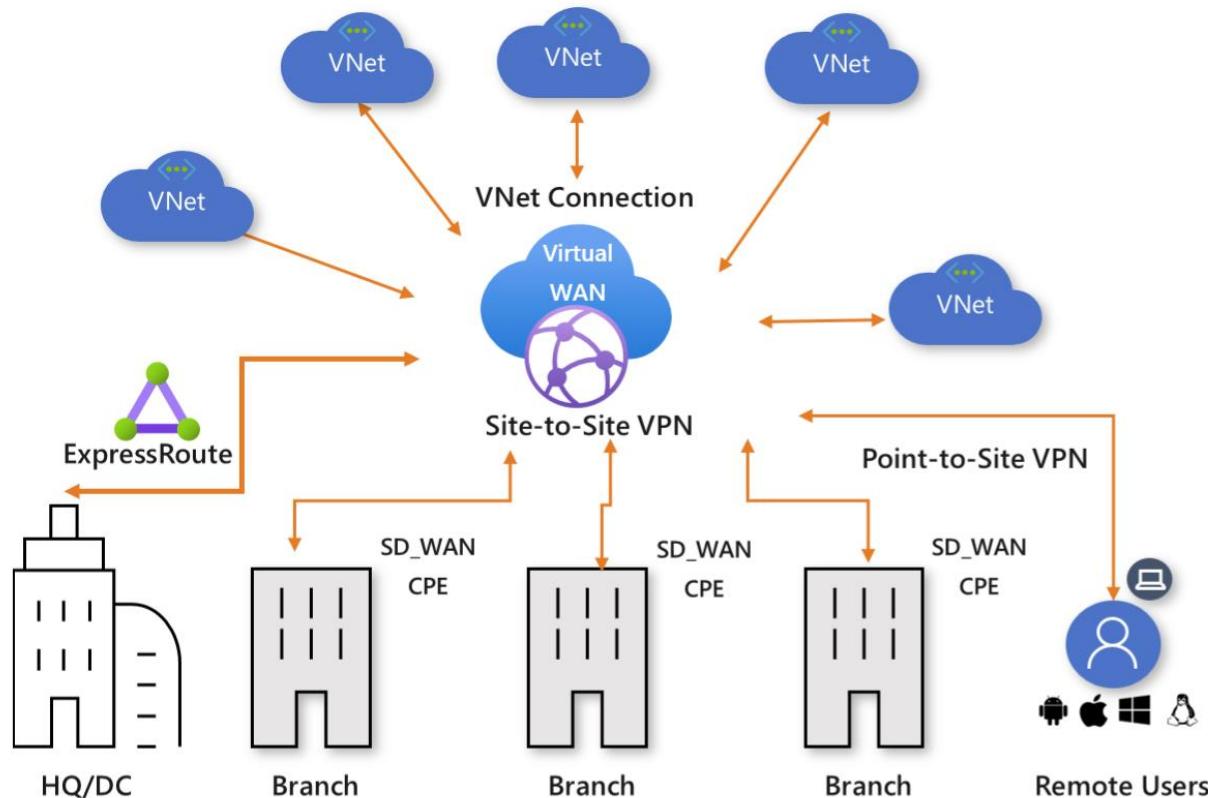
Any-to-any connectivity

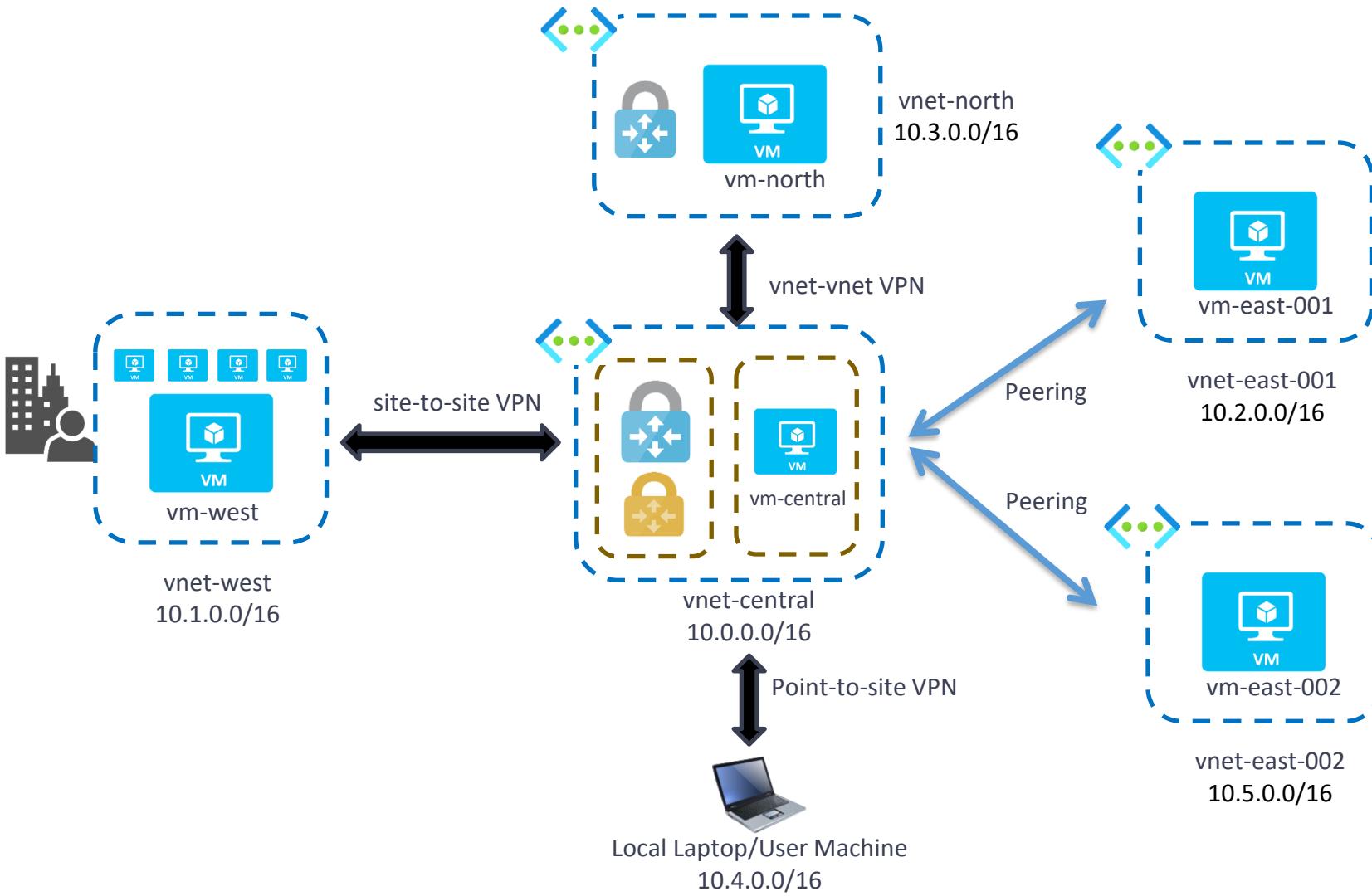


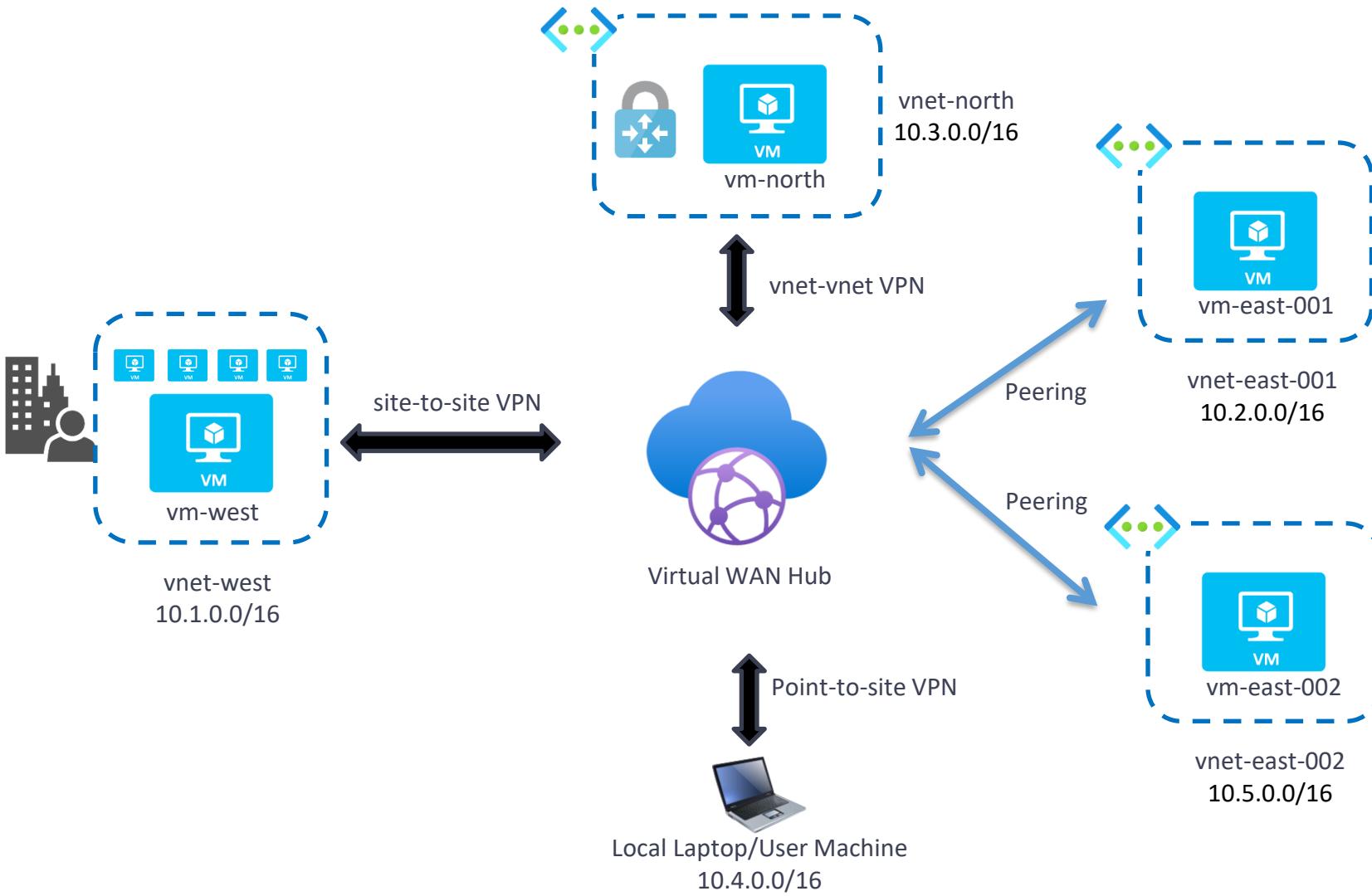
ExpressRoute

Fast, reliable, and private connection to Azure

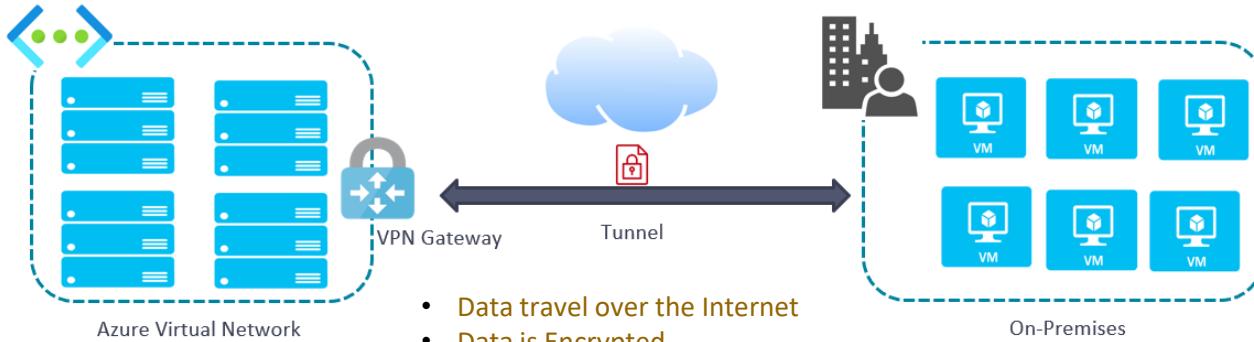
Virtual WAN



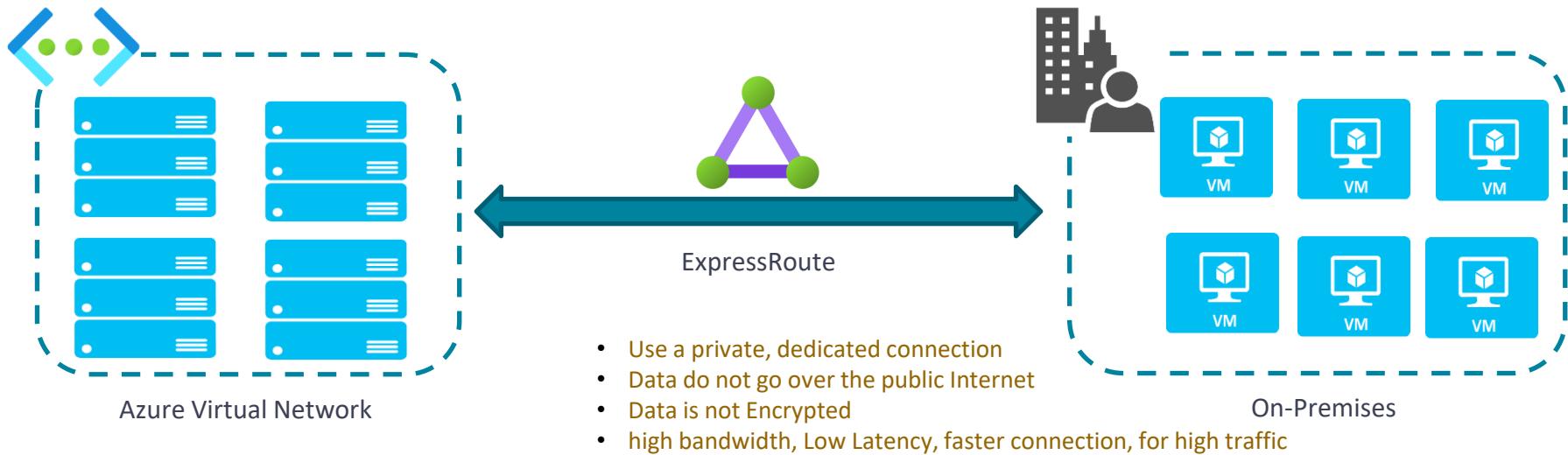




ExpressRoute



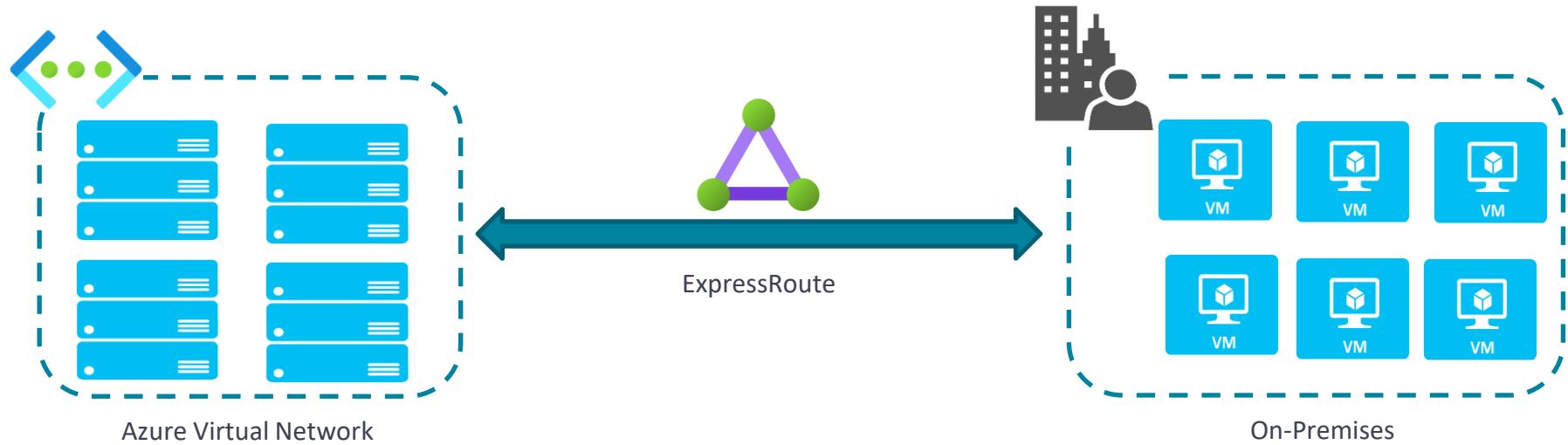
- Data travel over the Internet
- Data is Encrypted
- Slow connection, Latency, use for light traffic



- Use a private, dedicated connection
- Data do not go over the public Internet
- Data is not Encrypted
- high bandwidth, Low Latency, faster connection, for high traffic

On-Premises

ExpressRoute

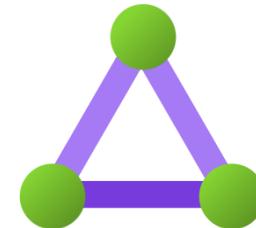


- Create private connections between Azure datacenters and infrastructure on your on-premises
- Offer more reliability, faster speeds, and lower latencies
- The setup and configuration for ExpressRoute is more complex, and will require collaboration with the connectivity provider.
- Large-scale, mission-critical workloads requiring scalability and resilience are suitable for this architecture.

ExpressRoute vs VPN Gateway

➤ ExpressRoute:

- Suitable for requirement for a high speeds, low-latency connection and high level of availability/resiliency.
- Suitable for mission critical workload.
- Access to all Azure services.
- Doesn't suit smaller satellite offices that have a lower connectivity requirement.

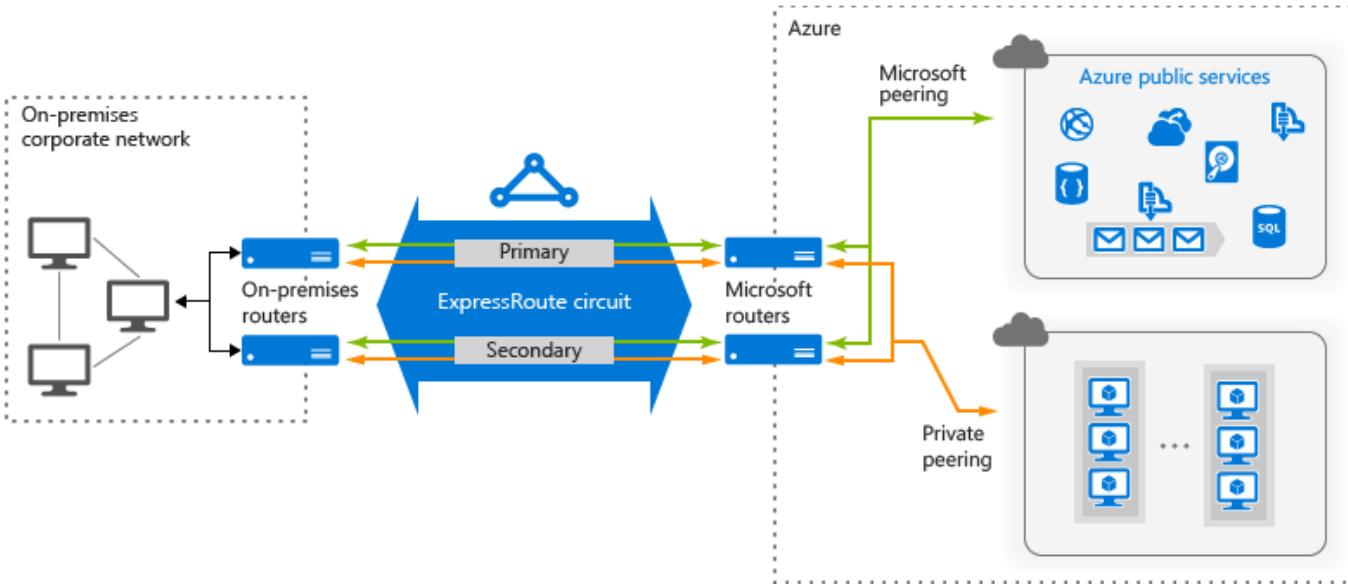


➤ VPN Gateway:

- Suitable for prototyping, development, test, labs, and small production workloads.
- Suitable for the small organization.
- VPN isn't designed to handle high data volumes.

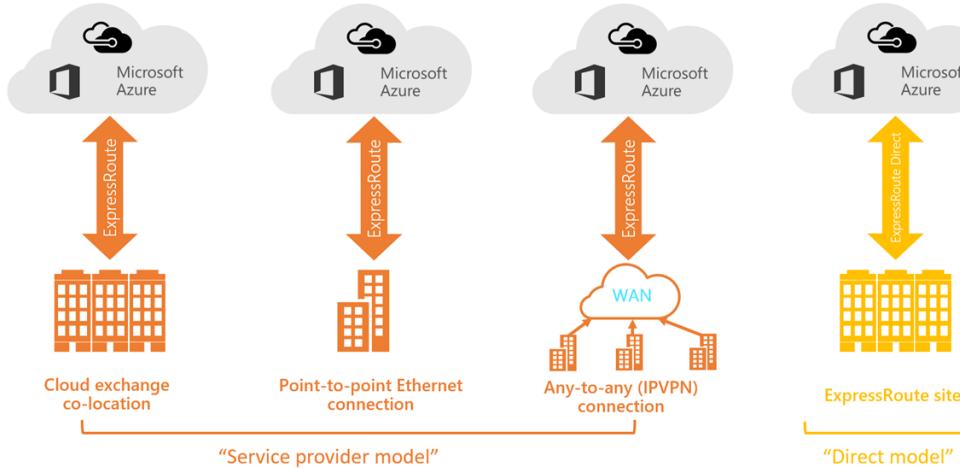


ExpressRoute Architecture



- An ExpressRoute circuit represents a logical connection between your on-premises infrastructure and Microsoft cloud services through a connectivity provider
- To get the high availability SLA, connect at least two routers to your on-premises corporate network and Microsoft Edge.
- ExpressRoute Peering
 - Private peering domain: Azure virtual networks, connect to compute services, namely virtual machines (IaaS) and cloud services (PaaS)
 - Microsoft peering: Microsoft 365, Dynamic 365, Azure public services (Public IPs)

ExpressRoute connectivity models



- **Cloud Exchange co-location:** use this to order virtual cross-connections to the Azure cloud through the co-location provider's Ethernet exchange. You need to bring your own routers to your service provider's datacenter and coming into the Microsoft Edge.
- **Point-to-Point Ethernet connection:** connect on-premises data centers to the Azure cloud through individual point-to-point links.
- **Any-to-Any connection:** designed for integrating an on-premises WAN with the Azure cloud. The connection to the Azure cloud looks just like any other branch office.
- **Direct from ExpressRoute site:** You can connect to Microsoft's worldwide network at a peering site. This enables Active/Active scaling at 100 Gbps or 10 Gbps.

Network Watcher

Network performance monitoring and diagnostics solution

Network Watcher

- Set of monitoring tools.
 - Focused on troubleshooting Azure Virtual Network issues
- Designed for network health of IaaS products which includes Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc.
 - Not work for PaaS monitoring or Web analytics.
- Three major sets of capabilities
 - Monitoring
 - Diagnostics
 - Metrics & Logging
- Monitor, diagnose and solve issues related to performance, connectivity, security, etc
 - VNet traffic filtering problems
 - Network routing problems
 - Hybrid cloud connectivity issues related to Gateway or Express Route
- Every region has a unique Network Watcher instance.
- The hidden NetworkWatcherRG resource group contains Network Watcher resources.



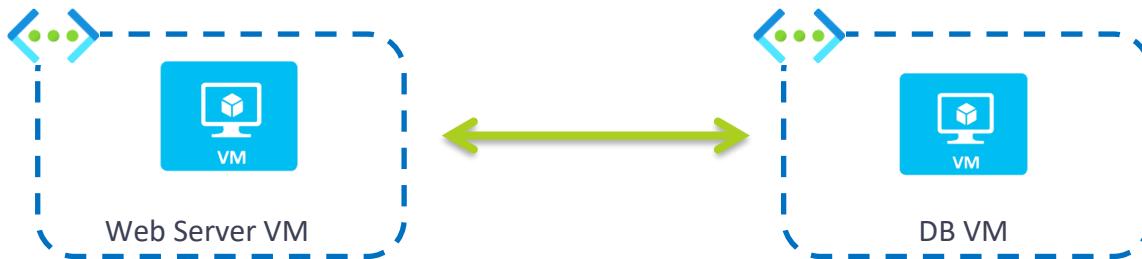
Connection Troubleshoot

- The connection troubleshoot capability enables you to test a point in time connection between a VM and another VM, an FQDN, a URI, or an IPv4 address.



Connection Monitor

- Connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint.
- Potential reasons are a DNS name resolution problem, the CPU, memory, or firewall within the operating system of a VM, or the hop type of a custom route, or security rule for the VM or subnet of the outbound connection.
- Provides the minimum, average, and maximum latency observed over time.
- Can send you alerts



Connection Monitor

Status
Reachable

Show data for last **1 hour** 6 hours 12 hours 1 day 7 days 30 days

Avg. Round-Trip Time and % Probes Failed

The chart displays two metrics over a period from 03:30 to 04:15. The Y-axis represents time in milliseconds (ms), ranging from 0ms to 1.0ms. The X-axis shows time points at 03:30, 03:45, 04 PM, and 04:15. A blue line represents the average round-trip time, which remains constant at 1.0ms. A purple line represents the percentage of probes failed, which remains at 0%. Both lines are plotted against a background grid.

Time	Avg. Round-Trip Time (ms)	% Probes Failed (%)
03:30	1.0	0
03:45	1.0	0
04 PM	1.0	0
04:15	1.0	0

AVG. ROUND-TRIP T...
MYVM1-MYVM2(22)
1.0 ms

% PROBES FAILED (...
MYVM1-MYVM2(22)
0 %

Grid view **Graph view**

Hops

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS	RTT FROM SOURCE (MS)
myvm1211	10.0.0.4	✓	10.0.0.5	0
myvm2529	10.0.0.5	✓	-	-

IP Flow

- IP Flow Verify Purpose: Checks if a packet is allowed or denied to or from a virtual machine.
 - For example, confirming if a security rule is blocking ingress or egress traffic to or from a virtual machine.
- Based on 5-tuple - specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound).
- IP flow verify tests the communication and reports success or failure.
- IP flow verify tells you which security rule allowed or denied the communication if the connection fails.

VPN Troubleshoot

- VPN diagnostics diagnoses the gateway's health and availability.
- VPN diagnostics tells you why the gateway or connection isn't working so you can fix it.

Network Watcher - VPN Diagnostics

Start troubleshooting

Network Watcher VPN Troubleshoot diagnoses the health of the virtual network gateway or connection. This request is a long running transaction, and the results are returned once the diagnosis is complete. You can select multiple gateways or connections to troubleshoot simultaneously. [Learn more.](#)

Choose a subscription: Resource group:

Storage account: [https://mysavpndiag.blob.core...](https://mysavpndiag.blob.core.windows.net/)

NAME	TROUBLESHOOTING ST...	RESOURCE STATUS	RESOURCE GROUP	LOCATION
<input checked="" type="checkbox"/> VNet1GW	Not started	Succeeded	TestRG1	East US
<input type="checkbox"/> VNet1toSite1	-	Succeeded	TestRG1	East US

Details

Status Action

Resource: [VNet1GW](https://myvpndiagnostics.blob.core.windows.net/vpndiagnostics)
Storage path: <https://myvpndiagnostics.blob.core.windows.net/vpndiagnostics>

Summary: Your VPN connectivity is impacted because the S2S VPN tunnels are disconnected
Detail: The S2S VPN tunnels could not connect because of IKE or connectivity issues

Status Action

Resource: VNet1GW

NAME	TROUBLESHOOTING STATUS	RESOURCE STATUS	RESOURCE GROUP	LOCATION
<input checked="" type="checkbox"/> VNet1GW	✖ Unhealthy	Succeeded	TestRG1	East US
<input type="checkbox"/> VNet1toSite1	-	Succeeded	TestRG1	East US

Details

Status Action

Resource: [VNet1GW](https://myvpndiagnostics.blob.core.windows.net/vpndiagnostics)
Storage path: <https://myvpndiagnostics.blob.core.windows.net/vpndiagnostics>

Summary: Your VPN connectivity is impacted because the S2S VPN tunnels are disconnected
Detail: The S2S VPN tunnels could not connect because of IKE or connectivity issues

Status Action

Check health of each individual connection to get more details
contact support
If your VPN gateway isn't up and running by the expected resolution time, contact support
<http://azure.microsoft.com/support>

Packet Capture

- Track traffic to and from a virtual machine.
- Helps to diagnose network anomalies both reactively and proactively.

The screenshot shows a NetworkMiner capture window titled "Microsoft: Wi-Fi". The main pane displays a list of network packets, each with columns for No., Time, Source, Dest. Port, Protocol, Length, DNS Time, TCP Delta, and Info. The "Info" column provides detailed TCP header information. A sidebar on the left lists flags and their meanings, with "SYN, ACK" selected. The bottom pane shows the raw hex and ASCII data for the selected packet (packet 2560). The status bar at the bottom indicates 12245 total packets, 316 displayed, and 0 dropped.

* Microsoft: Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1

No.	Time	Source	Dest. Port	Protocol	Length	DNS Time	TCP Delta	Info
2219	2017-02-14 07:31:26.221,183	1515.192.168.1.183	443 TCP	66	0.0000000000	1515>443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
2220	2017-02-14 07:31:26.264	23.100.86.91	443 192.168.1.183	1515 TCP	66	0.0431920000	443>1515 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2388	2017-02-14 07:31:30.176	23.100.86.91	443 TCP	66	0.0000000000	1520>443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
2390	2017-02-14 07:31:30.216	23.100.86.91	443 192.168.1.183	1524 TCP	66	0.0462750000	443>1520 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2470	2017-02-14 07:31:30.216	1512.192.168.1.183	443 TCP	66	0.0000000000	1521>443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1		
2471	2017-02-14 07:31:30.216	1512.192.168.1.183	443 192.168.1.183	1524 TCP	66	0.0431920000	443>1521 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2560	2017-02-14 07:31:37.304	192.168.1.183	1523 204.79.197.200	88 TCP	66	0.0000000000	1523>88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2561	2017-02-14 07:31:37.304	192.168.1.183	1524 204.79.197.200	88 TCP	66	0.0000000000	1524>88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2562	2017-02-14 07:31:37.395	204.79.197.200	89 192.168.1.183	1523 TCP	66	0.0016700000	89>1523 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2564	2017-02-14 07:31:37.398	204.79.197.200	89 192.168.1.183	1524 TCP	66	0.0015180000	89>1524 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2574	2017-02-14 07:31:37.465	192.168.1.183	1525 204.79.197.200	88 TCP	66	0.0000000000	1525>88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2575	2017-02-14 07:31:37.465	192.168.1.183	1526 204.79.197.200	88 TCP	66	0.0000000000	1526>88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2576	2017-02-14 07:31:37.467	204.79.197.200	89 192.168.1.183	1525 TCP	66	0.0019320000	89>1525 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2578	2017-02-14 07:31:37.467	204.79.197.200	89 192.168.1.183	1526 TCP	66	0.0016000000	89>1526 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2583	2017-02-14 07:31:37.487	192.168.1.183	1527 204.79.197.200	443 TCP	66	0.0000000000	1527>443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2584	2017-02-14 07:31:37.488	192.168.1.183	1528 204.79.197.200	443 TCP	66	0.0000000000	1528>443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2585	2017-02-14 07:31:37.489	204.79.197.200	443 192.168.1.183	1527 TCP	66	0.0016460000	443>1527 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2587	2017-02-14 07:31:37.489	204.79.197.200	443 192.168.1.183	1528 TCP	66	0.0015420000	443>1528 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
2570	2017-02-14 07:31:37.835	192.168.1.183	1529 204.79.197.200	443 TCP	66	0.0000000000	1529>443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	

Flags: 0x012 (SYN, ACK)

000... = Reserved: Not set
....0 = Nonce: Not set
....0 = Congestion Window Reduced (CWR): Not set
....0 = ECN-Echo: Not set
....0 = Urgent: Not set
....1 = Acknowledgment: Set
....0 = Push: Not set
....0 = Reset: Not set
>01 = Syn: Set
....00 = Fin: Not set
[TCP Flags:A-S]
Window size value: 8192
[calculated window size: 8192]
Checksum (tcp): Unverified
[Checksum Status: Unverified]
Urgent pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

> [SEQ/ACK analysis]

[This is an ACK to the segment in frame: 2560]
[The RTT to ACK in the segment was: 0.001687000 seconds]
[IRTT: 0.002110000 seconds]

> [timestamps]

0000 44 85 00 bf 03 6f c0 56 27 d3 44 fa 08 00 45 00 D...o.V ..D..E.
0010 00 34 7f d0 48 00 79 06 2d cc 4f c5 c8 c0 a8 .4..@y ..O...
0020 01 67 00 50 05 f3 e9 be f9 08 0f 32 3e f0 00 12 .g.P....23...
0030 2d 00 cc 67 00 08 02 04 05 a8 01 03 63 08 01 01 ..g.....
0040 04 02 ..

TCP Segment Len (tcp.len), 1 byte

Packets: 12245 - Displayed: 316 (2.6%) - Dropped: 0 (0.0%)

Profile: Default

Source: <https://docs.microsoft.com/>

Network Monitoring Logs

- NSG flow logs record source and destination IP addresses, ports, protocols, and whether traffic was allowed or denied.
- Traffic analytics can analyze logs and provide rich visualizations

Azure data centers with... ⓘ

7

out of 36

Active ports on inte... ⓘ

6

Hosts active on inte... ⓘ

26

Malicious flows ⓘ

2.87k

Allowed ⓘ 103
Blocked 2.77k

Traffic distribution across Azure data centers ⓘ

Active DCs 3

Inactive DCs 4

Allowed malicious... ⓘ

1/7

DCs affected

Traffic analytics enabl... ⓘ

Total 6

Active countries ⓘ

Total 147



Virtual network distribu... ⓘ

VNet traffic ⓘ Ex

Total 89 Or

Active 14 Az

Inactive 75 Pu

[Click here to see VNet traffic topol...](#)

[Click here to see live geomap](#)

Hosts with most traffic

4.5M

Total flows

IP	%	DISTRIBU...
----	---	-------------

10.156.1.4	9.02	
------------	------	---

10.186.1.4	7.4	
------------	-----	---

Most frequent conversations

4.5M

Total flows

SOURCE	DESTI...	%	DISTRI...
--------	----------	---	-----------

10.186...	10.15...	3.33	
-----------	----------	------	---

westus2	10.4.1.4	1.46	
---------	----------	------	---

Top application protocols

4.5M

Total flows

L7 PROTO...	%	DISTRIBU...
-------------	---	-------------

http	6.06	
------	------	---

ldap	1.43	
------	------	---

Network Monitoring Logs

- NSG flow logs record source and destination IP addresses, ports, protocols, and whether traffic was allowed or denied.
- Traffic analytics can analyze logs and provide rich visualizations
- Traffic analytics provides the following information:
 - Most-communicating hosts
 - Most-communicating application protocols
 - Most-conversing host pairs
 - Allowed and blocked traffic
 - Inbound and outbound traffic
 - Open internet ports
 - Most-blocking rules
 - Traffic distribution per Azure datacenter, virtual network, subnets, or rogue network

Network Watcher Tools

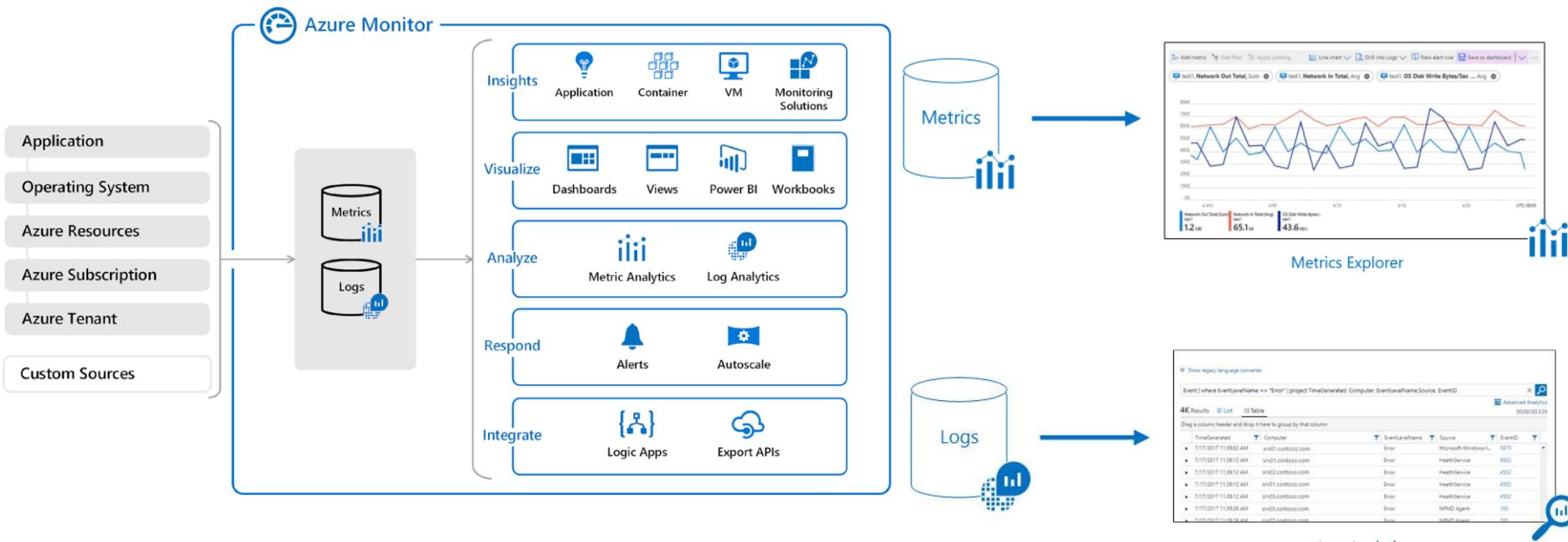
- Monitoring
 - **Topology** view shows you the resources in your virtual network and the relationships between them.
 - **Connection Monitor** allows you to monitor connectivity and latency between a VM and another network resource.
 - **Network performance monitor** allows you to monitor connectivity and latencies across hybrid network architectures, Expressroute circuits, and service/application endpoints.
- Diagnostics
 - **IP Flow Verify** allows you to detect traffic filtering issues at a VM level.
 - **Next Hop** helps you verify traffic routes and detect routing issues.
 - **Connection Troubleshoot** enables a one-time connectivity and latency check between a VM and another network resource.
 - **Packet Capture** enables you to capture all traffic on a VM in your virtual network.
 - **VPN Troubleshoot** runs multiple diagnostics checks on your VPN gateways and connections to help debug issues.
- Logging
 - **NSG Flow Logs** allows you to log all traffic in your Network Security Groups (NSGs)
 - **Traffic Analytics** processes your NSG Flow Log data enabling you to visualize, query, analyze, and understand your network traffic.

Azure Monitor

Full observability into your applications, infrastructure, and network

Azure Monitor

- Collect, Analyze, Visualize and take actions based on metric and logging data
- Collect data from Cloud and On-premises infrastructure



Azure Monitor - 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](#)



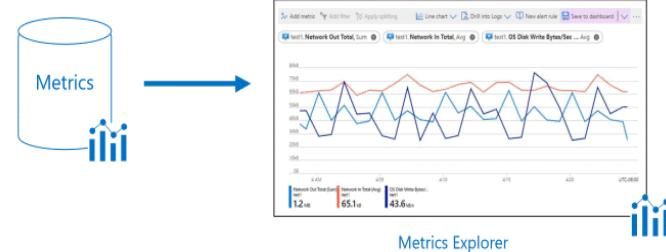
Setup Alert & Actions

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

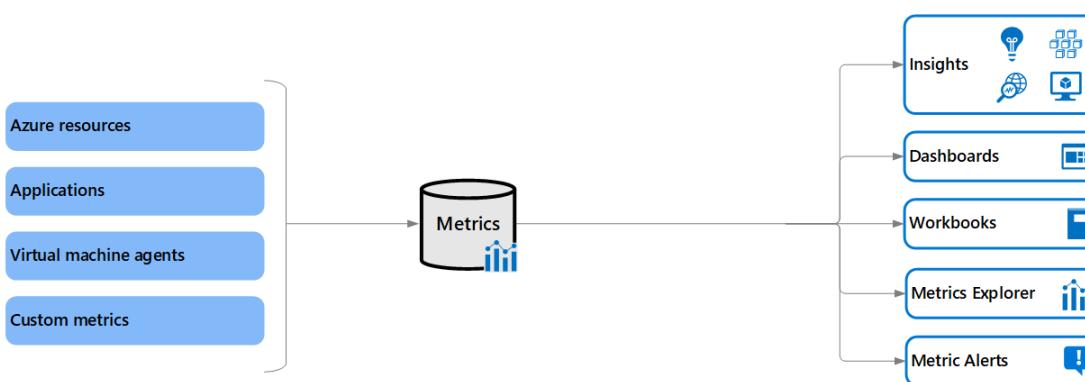
[Create Alert](#)

Azure Monitor - Metrics

- Collect numeric data at regular intervals into time-series database.
- lightweight and capable of supporting near-real-time scenarios.
- What you can do with them?
 - Analyze them interactively by using Metrics Explorer.
 - Be proactively notified with an alert when a value crosses a threshold.
 - Visualize them in a workbook or dashboard.
- Azure resources Overview page displays Azure Monitor data for many resources.
- Metrics can be accessed from the Azure Portal, the Monitor REST and .Net APIs, and analysis tools like Log Analytics and Event Hubs.



Metrics Explorer



Azure Monitor Logs

➤ Resource Logs

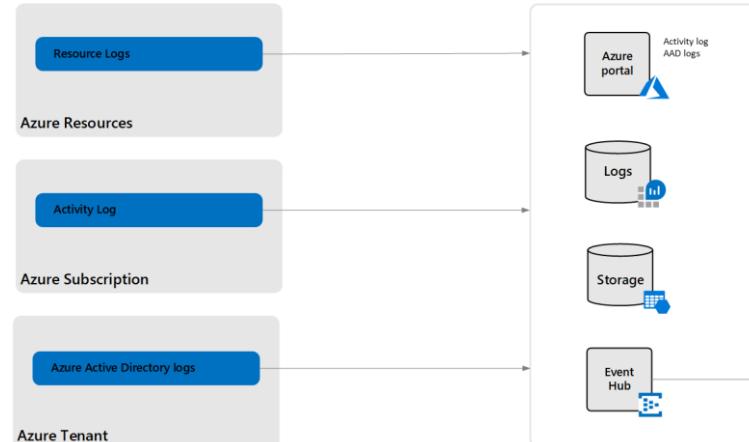
- Layer: Azure Resources
- Provide insight into operations that were performed within an Azure resource (the data plane).
- Examples: for SQL Server: Error, Timeout, Deadlock.
- The content of resource logs varies by the Azure service and resource type.

➤ Activity Log

- Layer: Azure Subscription
- Provides insight into the operations on each Azure resource in the subscription from the outside (the management plane)
- Also included Service Health events
- Use the Activity log to determine the what, who, and when for any write operations

➤ Azure Activity Directory Logs:

- Contain the history of sign-in activity and audit trail of changes made in Azure AD for a particular tenant.



Azure Monitor - Resource Logs

- Provide insight into operations that were performed within an Azure resource (the data plane).
- Azure resources generate logs automatically, but NOT collected without a diagnostic setting.
 - Without storing logs, you cannot even view them.
- Diagnostic setting destinations
 - **Log Analytics workspace:** Like a Datawarehouse, data repository, for more complex querying and alerting.
 - **Azure Event Hubs:** Optimized for telemetry data, great when you are building event pipelines, forward outside of Azure
 - **Azure Storage:** cheaper, long term retention, archival store, compliance purpose.
 - **Partner solution:** Specialized integrations between Azure Monitor and other non-Microsoft monitoring platforms.
- Resource, Event Hub, and Azure Storage must be in the same region.
- Log content varies by Azure service and resource type.
- Resource log tables vary by collection type.
 - **Azure diagnostics:** All data is written to the AzureDiagnostics table.
 - **Resource-specific:** Data is written to individual tables for each category of the resource.
 - All Azure services will eventually migrate to the resource-specific mode.
- Resource logs were previously referred to as diagnostic logs.

Azure Monitor - Activity log

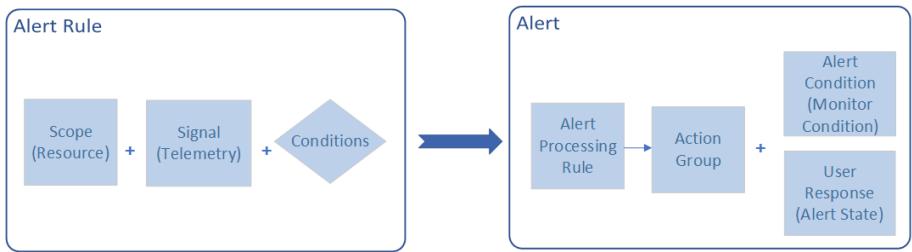
- Provides insight into subscription-level events.
- Includes information like when a resource is modified or property change at the service level
 - Example: Virtual machine is started/stopped or Size changed or tier changed
- Activity Log events are stored for 90 days. To store this data for longer periods, export it to Storage Account, Log Analytics or Event Hubs.
- Activity logs you send to a Log Analytics workspace are stored in a table called AzureActivity.

The screenshot shows the Azure Monitor - Activity log interface. On the left, there's a navigation sidebar with links like Overview, Activity log (which is selected), Alerts, Metrics, Logs, Service Health, Workbooks (preview), Insights (Applications, Virtual Machines (preview), Containers, Network, More), Settings (Diagnostics settings, Autoscale), and Support + Troubleshooting. The main area has a search bar and filter options (Management Group: None, Subscription: Contoso IT - demo, Timespan: Last 6 hours, Event severity: All, Add Filter). Below these are buttons for Edit columns, Refresh, Export to Event Hub, Download as CSV, Logs, Pin current filters, and Reset filters. The main content area displays a table titled 'First 75 items.' with columns: OPERATION NAME, STATUS, TIME, TIME STAMP, SUBSCRIPTION, and EVENT INITIATED BY. The table lists various events such as Create or Update Virtual Machine, Append, DeployIfNotExists, DeployIfNotExists, Create or Update Virtual Machine, Create or Update Virtual Machine, Create or Update Virtual Machine Extension, Create Deployment, Create Deployment, DeployIfNotExists, Returns Storage Account SAS Token, and Validate Deployment, all from the Contoso IT - demo subscription and initiated by Microsoft Azure Policy Insights or Windows Azure Application Insights.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Create or Update Virtual Machine	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	
Append	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	Microsoft Azure Policy Insights
DeployIfNotExists	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	Microsoft Azure Policy Insights
DeployIfNotExists	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	Microsoft Azure Policy Insights
Create or Update Virtual Machine	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	
Create or Update Virtual Machine	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	
Create or Update Virtual Machine Extension	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	
Create Deployment	Failed	3 min ago	Sat May 11 ...	Contoso IT - demo	
Create Deployment	Failed	3 min ago	Sat May 11 ...	Contoso IT - demo	
DeployIfNotExists	Failed	4 min ago	Sat May 11 ...	Contoso IT - demo	
Returns Storage Account SAS Token	Succeeded	5 min ago	Sat May 11 ...	Contoso IT - demo	Windows Azure Application Insights
Validate Deployment	Succeeded	6 min ago	Sat May 11 ...	Contoso IT - demo	

Azure Monitor - Alerts

- Alerts proactively notify you when Azure Monitor data indicates that there may be a problem with your infrastructure or application.
- They allow you to identify and address issues before the users of your system notice them.
- You create an alert rule by combining:
 - The resource(s) to be monitored.
 - The signal or telemetry from the resource
 - Conditions
- Once an alert is triggered, the alert is made up of:



- **Action Group:** can trigger notifications or an automated workflow to let users know that an alert has been triggered.
 - Various alerts may use the same or different action groups based on user needs.
- **Alert Processing Rule:** You can add or suppress action groups, apply filters, or schedule alert processing rules.
- **Alert Condition:** set by system (Fired, resolved)
- **Alert State:** set by the user
 - **New:** The issue has been detected and has not yet been reviewed.
 - **Acknowledged:** An administrator has reviewed the alert and started working on it.
 - **Closed:** The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.

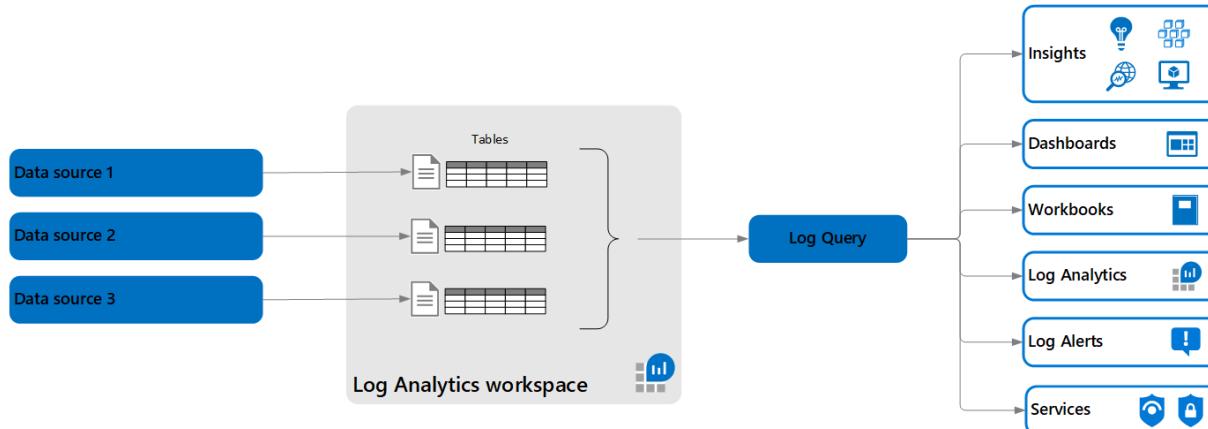
Azure Monitor - Alerts Types

There are four types of alerts:

- Metric alerts
 - evaluates conditions on the resource metrics at regular intervals
 - NOT Free, charged based on the number of time-series that are monitored.
- Log alerts
 - monitors a resource by using a Log Analytics query
 - NOT Free
- Activity log alerts
 - monitors a resource by checking the activity logs
 - FREE
- Smart detection alerts
 - Smart Detection monitors the data received from your app, and in particular the failure rates.
 - It uses machine learning algorithms to predict the normal failure rate.
 - App Insights alerts you in near real time if your web app experiences an abnormal rise in the rate of failed requests.

Log Analytics (Azure Monitor Logs)

- A separate Azure resource which act like a container for logs.
- Helps you collect and analyze data generated by resources in your cloud and on-premises environments.
- Logs are handled not meaningless strings of text, but instead organized in well defined schemas, helps analyze the data properly and efficiently.
- Workspace can handle terabytes of data per day.
- Log Management: example RBAC, retention, policies and more
- Log Exploration: including non-azure resources (example on-premises vm)



Azure Application Insights

- Provides application performance management (APM) and monitoring for live web apps.
- Azure Monitor vs Application Insight
 - Azure Monitor metrics, alerts and logs -> Azure Infrastructure (performance and troubleshooting and optimization)
 - Application Insights -> Business Application performance
- Developers and DevOps professionals can use Application Insights to:
 - Automatically detect performance anomalies.
 - Help diagnose issues by using powerful analytics tools.
 - See what users actually do with apps.
 - Help continuously improve app performance and usability.
- Application Insights:
 - Supports a wide variety of platforms, including .NET, Node.js, Java, and Python.
 - Works for apps hosted on-premises, hybrid, or on any public cloud.
 - Integrates with DevOps processes.
 - Has connection points to many development tools.
 - Can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

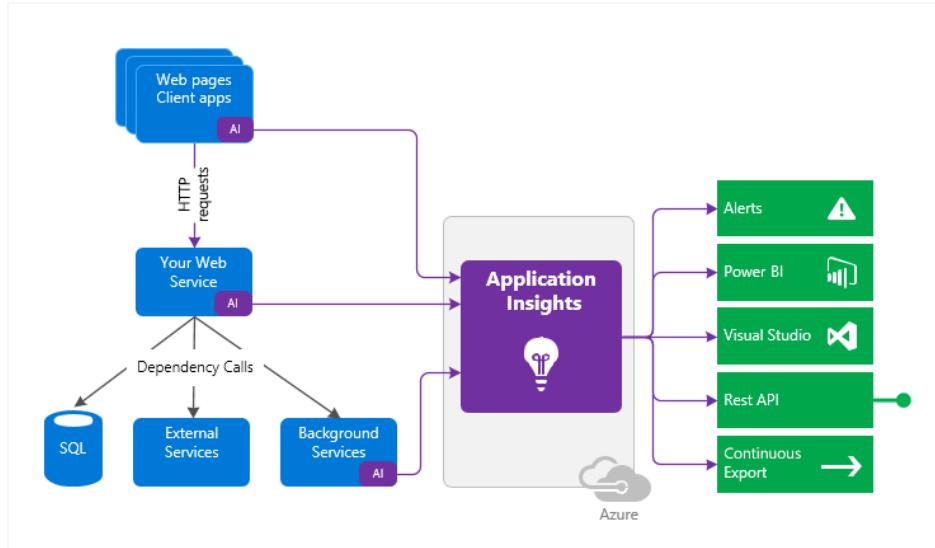


Application Insights

How Application Insights works

- Install a small instrumentation package (SDK) in your application or enable Application Insights using the Application Insights Agent when supported.
- The instrumentation monitors your app and directs the telemetry data to an Azure Application Insights

Small Instrument Package (SDK) →



What Application Insights monitors?

- **Request rates, response times, and failure rates** - Find out which pages are most popular, at what times of day, and where your users are. See which pages perform best. If your response times and failure rates go high when there are more requests, then perhaps you have a resourcing problem.
- **Dependency rates, response times, and failure rates** - Find out whether external services are slowing you down.
- **Exceptions** - Analyze the aggregated statistics, or pick specific instances and drill into the stack trace and related requests. Both server and browser exceptions are reported.
- **Page views and load performance** - reported by your users' browsers.
- **AJAX calls from web pages** - rates, response times, and failure rates.
- **User and session counts**.
- **Performance counters** from your Windows or Linux server machines, such as CPU, memory, and network usage.
- **Host diagnostics** from Docker or Azure.
- **Diagnostic trace logs from your app** - so that you can correlate trace events with requests.
- **Custom events and metrics** that you write yourself in the client or server code, to track business events such as items sold or games won.



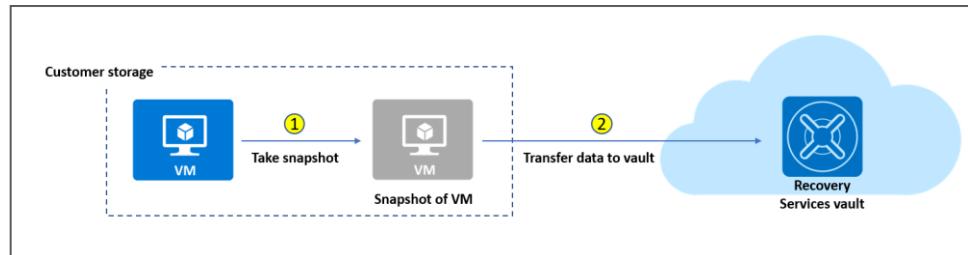
Application Insights

Backup vs Disaster Recovery

- **Disaster Recovery:** After a catastrophic failure, you must run your sites, servers, or applications in Azure secondary datacenter.
 - **Azure Site Recovery:** replicates the data in almost real time and allows for a failover.
- **Backup:** When your data is corrupted or lost and you need to restore it to original copy.
 - **Azure Backup Service:** maintain copies of stateful data that allow you to go back in time.
 - Granular data protection and restoration, you can restore only few corrupted files.
- **RTO vs RPO**
 - **Recovery Time Objective (RTO):** The time it takes to complete a recovery or restore.
 - **Recovery Point Objective (RPO):** The amount of acceptable data loss if a recovery is needed.

Azure Backup Service

- Allows you to back up Azure virtual machines, on-premises servers, Azure file shares, and SQL Server or SAP HANA running on Azure VMs, and other application workloads.
- Azure Backup uses a Recovery Services vault to manage and store the backup data.
- **Recovery Services vault** is a storage object in Azure
 - Designed for backup and recovery of Azure Resources.
 - Provide a central place for organizing and managing your backup continuity and disaster recovery strategy
 - Use for both Azure Backup and Azure Site Recovery.
 - Handles management tasks like reporting, site replication, backup, and restore.
 - Can be used for on-premises workloads in addition to workloads in AWS
 - Recovery service vault and source VM should be in same location



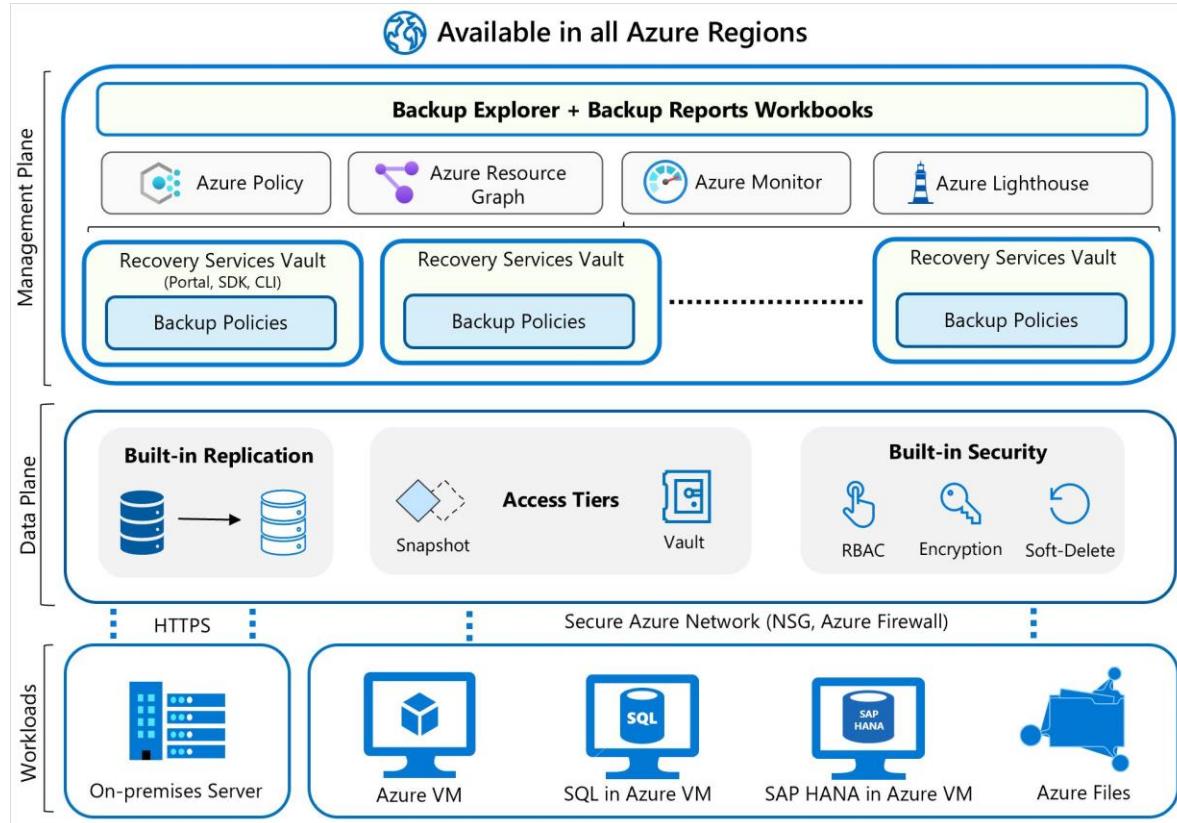
Snapshot Consistency

- Application consistent
 - The snapshot captures the VM as a whole. It uses VSS writers to capture the content of the machine memory and any pending I/O operations.
 - For Linux machines, you'll need to write custom pre or post scripts per app to capture the application state.
 - You can get complete consistency for the VM and all running applications.
- File system consistent
 - If VSS fails on Windows, or the pre and post scripts fail on Linux, Azure Backup will still create a file-system-consistent snapshot.
 - During a recovery, no corruption occurs within the machine. But installed applications need to do their own cleanup during startup to become consistent.
- Crash consistent
 - This level of consistency typically occurs if the VM is shut down at the time of the backup.
 - No I/O operations or memory contents are captured during this type of backup. This method doesn't guarantee data consistency for the OS or app.

Snapshot Consistency

- Application consistent
 - The snapshot captures the VM as a whole. It uses VSS writers to capture the content of the machine memory and any pending I/O operations.
 - For Linux machines, you'll need to write custom pre or post scripts per app to capture the application state.
 - You can get complete consistency for the VM and all running applications.
- File system consistent
 - If VSS fails on Windows, or the pre and post scripts fail on Linux, Azure Backup will still create a file-system-consistent snapshot.
 - During a recovery, no corruption occurs within the machine. But installed applications need to do their own cleanup during startup to become consistent.
- Crash consistent
 - This level of consistency typically occurs if the VM is shut down at the time of the backup.
 - No I/O operations or memory contents are captured during this type of backup. This method doesn't guarantee data consistency for the OS or app.

Azure Backup



Azure Backup features

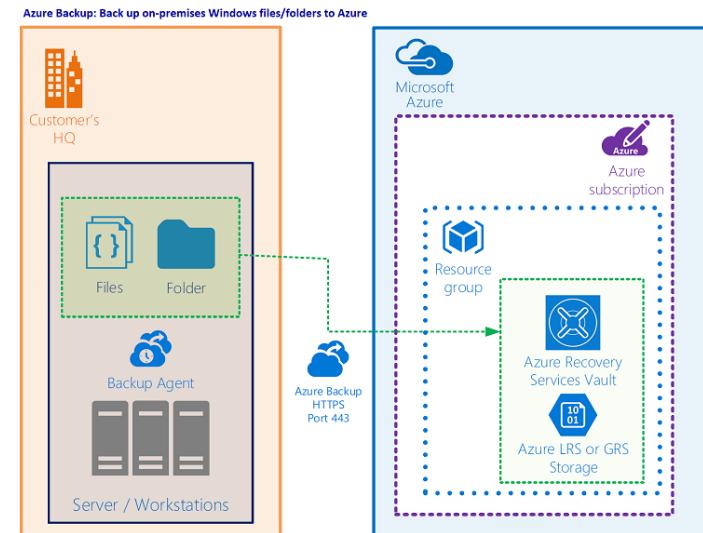
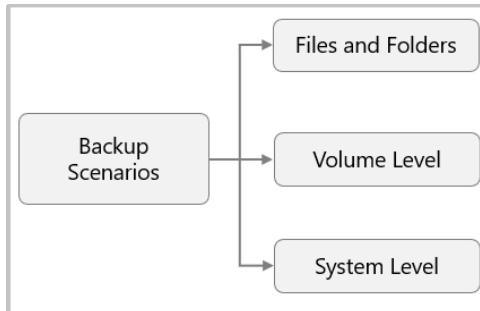
- **Zero-infrastructure backup:** Azure Backup eliminates the need to deploy and manage overhead of backup infrastructure or storage.
- **Long-term retention**
- **Security:** Azure Backup protects data in transit and at rest.
- **Azure role-based access control:** RBAC lets you segregate team duties and give users only the access they need.
- **Encryption of backups:** Microsoft-managed keys encrypt backup data. You can also encrypt backed-up data using customer-managed keys in Azure Key Vault.
- **Soft delete:** Soft delete keeps backup data for 14 days after deleting an item. This protects backups from accidental or malicious deletion, preventing data loss.
- **High availability:** Azure Backup offers three types of replication:
 - Locally redundant storage (LRS): Provides basic protection against server rack and drive failures. Non-critical situations are best.
 - Geo-redundant storage (GRS): Provides failover in a secondary region. It's great for backups.
 - Zone-redundant storage (ZRS): Provides datacenter-level failure protection. High availability is recommended.
- **Centralized monitoring and management:** Azure Backup's Recovery Services vault includes built-in monitoring and alerting. These capabilities are available without additional management infrastructure.

Backup Methods

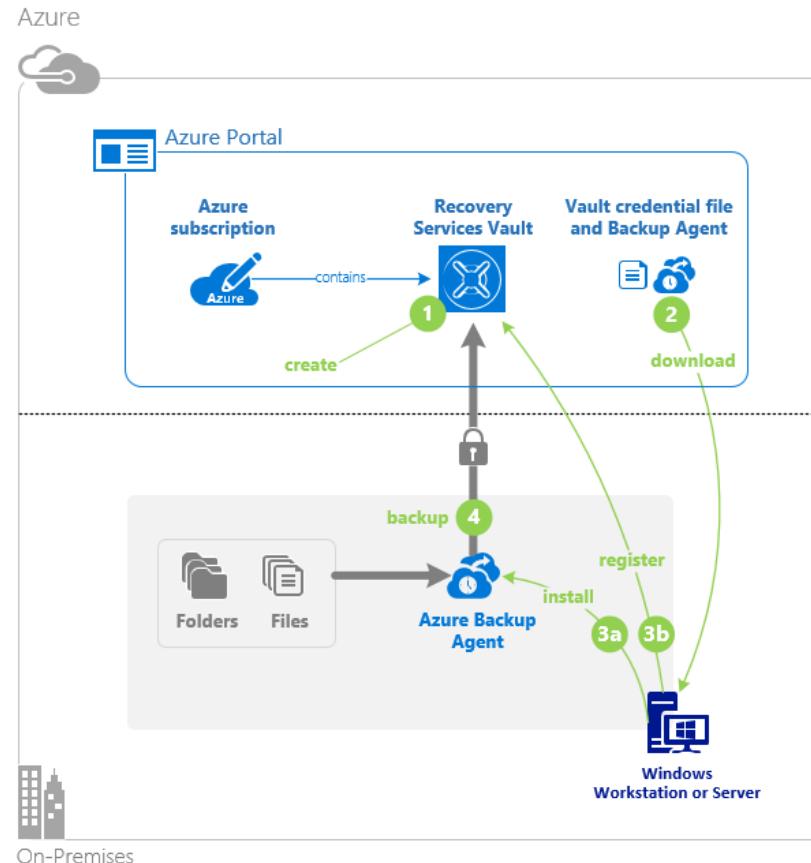
- **Azure VM backup**
 - Azure Backup service directly backs up Azure virtual machines (VMs).
 - Azure Backup adds a backup extension (VMSnapshot extension) to the Azure VM agent.
 - This method backs up the entire VM. If you want to back up specific files and folders on the VM, install and use the MARS agent alongside the extension.
- **MARS (Microsoft Azure Recovery Services)**
 - You can back up specific files and folders
 - You can backup both Azure VM or on-premises Windows Server machines by running the MARS agent.
- **DPM/MABS (Data Protection Manager/Azure Backup Server)**
 - On-premises machines can be backed up to DPM or Azure Backup Server (MABS). The backup server can be backed up to Azure Recovery Services.
 - You can back up Azure VMs to the MABS that's running in Azure, and you can then back up the MABS to a Recovery Services vault.

MARS agent

- The MARS agent uses VSS to take a point-in-time snapshot of the volumes selected for backup.
 - The MARS agent captures the snapshot using Windows system write.
 - The agent doesn't capture app-consistent snapshots because it doesn't use application VSS writers.
- Backup scenarios
 - Files and Folders: Selectively protect Windows files and folders.
 - Volume Level: Protect an entire Windows volume of your machine.
 - System Level: Protect an entire Windows system state



MARS (Microsoft Azure Recovery Services) agent



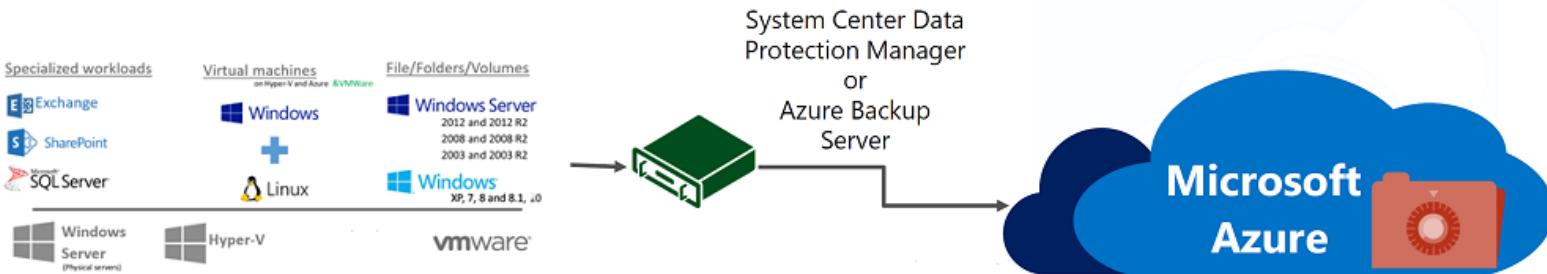
Azure VM backup options

- Azure VM backup by using VM extension
 - Directly backup Azure VMs. Azure Backup adds a backup extension to the Azure VM agent. This extension backs up VMs.
 - This method backs up the entire VM. If you want to back up specific files and folders on the VM, install and use the MARS agent alongside the extension.
- Azure VM backup by using MARS agent
 - You can back up specific files and folders on the Azure VM or on-premises Windows Server machines by running the MARS agent.
- Azure VM with DPM/MABS
 - On-premises machines can be backed up to DPM or Azure Backup Server (MABS). The backup server can be backed up to Azure Recovery Services.
 - You can back up Azure VMs to the MABS that's running in Azure, and you can then back up the MABS to a Recovery Services vault.

Back up to DPM/MABS

- You install the DPM or MABS protection agent on machines to protect. You then add the machines to a DPM protection group.
- DPM/MABS protects backups, shares, files, and folders. You can also protect bare metal and specific apps with app-aware backup.
- The DPM/MABS disks are backed up to the vault by the MARS agent that's running on the DPM/MABS server.

Azure Backup: Back up workloads (on-premises and on Azure VMs) protected by DPM or Microsoft Azure Backup Server (MABS)



Backup Report

- Help you get rich insights on your backups across your entire backup estate.
 - Allocating and forecasting of cloud storage consumed.
 - Auditing of backups and restores.
- Azure Backup leverages Azure Monitor logs and Azure workbooks for reporting.
- **Supported for** Azure VMs, SQL in Azure VMs, SAP HANA in Azure VMs, Microsoft Azure Recovery Services (MARS) agent, Microsoft Azure Backup Server (MABS), and System Center Data Protection Manager (DPM).
- Can be viewed **across all backup items, vaults, subscriptions, and regions** as long as their data is being sent to a Log Analytics workspace that the user has access to.

Backup Report- Summary

Overview Summary Backup Items Usage Jobs Policies

Report Filters

Filters are applied left to right and top to bottom on each page. [Learn More](#)

Time Range ⓘ

All datetimes are in UTC. Data for the current partial day is not shown in the reports. [Learn More](#)

Backup Items 42	Protected Instances 15.5	Cloud Storage (GB) 570.98	Jobs Created 33
--------------------	-----------------------------	------------------------------	--------------------

Key Parameters by Backup Item Type

Backup Management Type ↑↓	Backup Item Type ↑↓	# Backup...↑↓	Job Succ...↑↓	Cloud Sto...↑↓
Azure Backup Agent	Files and Folder	7	-	190.60
Azure Storage (Azure Files)	Azure File Share	1	100.0 %	0.00

Backup Report - Backup Items

Search item or Container ⓘ
Enter value

Protected: 82 | ProtectionStopped: 7 | InitialBackupPending: 2

Backup Items Trend

Backup Items (Last) 91

Cloud Storage Trend

Cloud Storage (GB) (Last) 1.68 k

Storage by BackupItem

Search Policy Name ⓘ Sort By ⓘ Order ⓘ Rows Per Page ⓘ Page ⓘ
Enter value Cloud Storage (MB) Descending 10 1 of 10

Backup Item	Container	Resource Group	Policy	Cloud Sto...	Vault	Storage Replication Type	Azure Resource
c:\	SONIA-LAPTOP.FAREAST.CORP.MICROSOFT.COM	(none)	MABPol01b8affd-9f34-4de1-bc8c-5b02197b486f	455.92	SOGUPVAULT	GeoRedundant	
sqlserver-1	sqlserver-1	shopkartdemo	FinanceTest	239.53	SHOPKARTDEMOVAULT	GeoRedundant	sqlserver-1
systemdb	hanamachine2	SAPHANA	SAPHANABackupPolicy	117.06	SAPHANAVALUT2	GeoRedundant	hanamachine2
hxe	hanamachine2	SAPHANA	SAPHANABackupPolicy	116.13	SAPHANAVALUT2	GeoRedundant	hanamachine2

Backup Report - Usage

Search Billed Entity ⓘ
Enter value

Azure Backup Agent Protected Instance Count 13	Azure Storage (Azure File... Protected Instance Count 0	Azure Virtual Machine Protected Instance Count 19.5	SAP HANA in Azure VM Protected Instance Count 4	SQL in Azure VM Protected Instance Count 1	LocallyRedundant Cloud Storage (GB) 13.49	GeoRedundant Cloud Storage (GB) 1,664.22
---	--	--	--	---	--	---

Protected Instances Trend

Protected Instances (Last) **37.5**

Cloud Storage Trend

Cloud Storage (GB) (Last) **1.68 K**

Protected Instances and Storage by Billed Entity

Sort By ⓘ Order ⓘ Rows per page ⓘ Page ⓘ

Billed Entity	Billed Entity Resource Group	Billed Entity Type	Backup Management Type	# Protect...	Cloud Sto...	Storage Replication Type	Vault	Vault Resource Group
SONIA-LAPTOP.FAREAST.CORP.MICROSOFT.COM (none)		ProtectedContainer	Azure Backup Agent	1	455.92	GeoRedundant	SOGUPVAULT	SOGUPBUGBASHRG
sqlserver-1	shopkartdemo	ProtectedContainer	Azure Virtual Machine	0.5	239.53	GeoRedundant	SHOPKARTDEMOVAULT	SHOPKARTDEMO

Backup Report - Jobs

Search Item or Container (Job Operation (Job Status (Job Failure Code (Enter value All All All All)))))

Success % Succeeded SucceededWithWarnings Failed Cancelled

96.97 32 0 1 0

Jobs by Status over Time

Date	Status	Count
Feb 4	Succeeded	5
Feb 5	Succeeded	5
Feb 6	Succeeded	5
Feb 7	Succeeded	5
Feb 9	Succeeded	5
Feb 9	Failed	1

Jobs by Job Operation

Operation	Count
Backup	33

Distribution of Jobs in Period by Backup Item

Sort By (Job Success %) Order (Ascending) Rows per Page (10) Page (1 of 5)

Backup Item	Container	Resource Group	# Jobs Failed	Job Success %	Avg Data... (Avg Job ...)	Azure Resource
utsvm1	UtsVm1	utsnetrg3	1	0.0 %	0.0	2.09
shopkartemp	ShopKartEmp	shopkartdemo	0	100.0 %	263.83	0.75
sqlserver-0	sqlserver-0	shopkartdemo	0	100.0 %	0.0	0.52
sqlserver-1	sqlserver-1	shonkartdemo	0	100.0 %	827.71	1.4

Backup Report - Policies

Search Policy Name ⓘ

Active Policies
Count
22

GeoRedundant
Cloud Storage (GB)
570.98

Active Policy Trend

Active Policies (Last)
22

Cloud Storage Trend

Cloud Storage (GB) (Last)
571

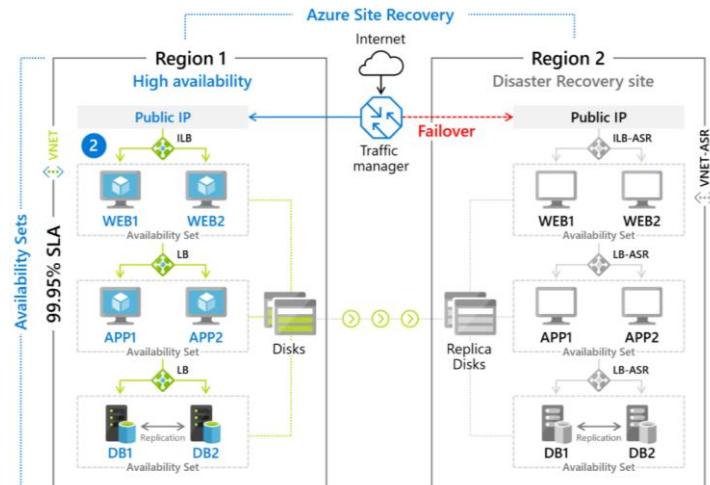
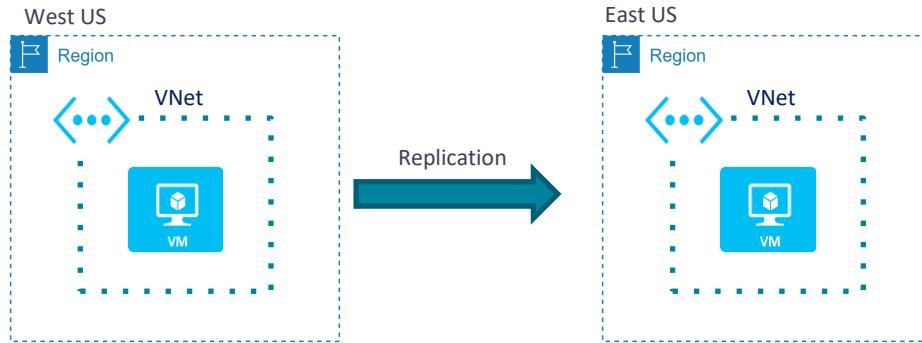
Backup Items and Storage by Policy

Sort By ⓘ Order ⓘ Rows Per Page ⓘ Page ⓘ
Vault Storage (MB) Descending 10 1 of 3

Policy Name	# Backup	Cloud Sto.	Vault	Storage Replication Type
FinanceTest	1	232.36	SHOPKARTDEMOVAULT	GeoRedundant
MABPol02299247-06e1-46ea-868b-e07a5b8ee1f0	1	89.41	SHOPKARTDEMOVAULT	GeoRedundant
DefaultPolicy	3	85.96	SHOPKARTDEMOVAULT	GeoRedundant
MABPol0fb340f1-ab66-4505-8838-ed0afa57974c	2	84.86	WACVAULT1	GeoRedundant

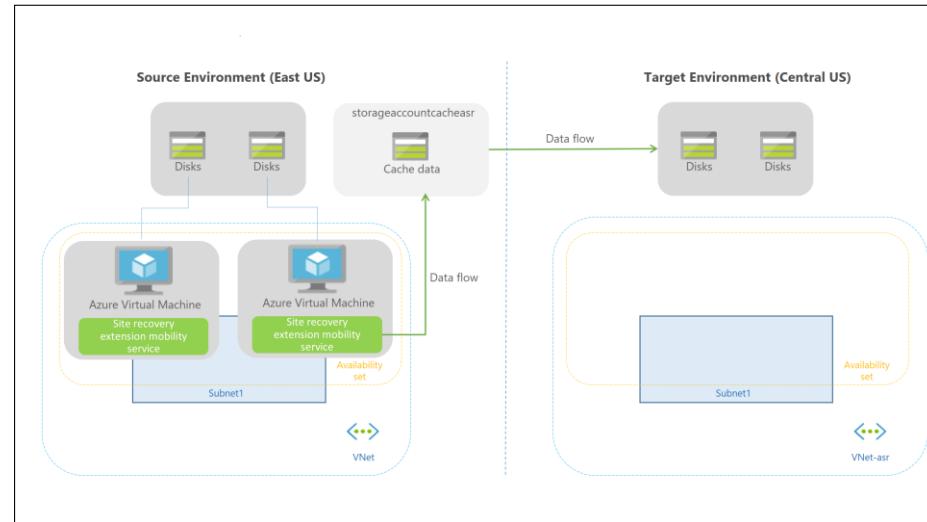
Azure Site Recovery

- Ensure business continuity and disaster recovery (BCDR)
- Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location.
- When an outage occurs at your primary site, you fail over to a secondary location, and access apps from there.
 - After the primary location is running again, you can fail back to it.
- Helps ensure business continuity by keeping business apps and workloads running during outages.
- You can replicate:
 - Azure VMs from a primary region to a secondary region.
 - VMware VMs to Azure
 - On-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter.
- Replication frequency as low as 30 seconds for Hyper-V
- Planned failovers for expected outages with zero-data loss.
- Unplanned failovers with minimal data loss, depending on replication frequency



Enable Replication Process (ASR)

- Target resource group may be in any region except the source VMs'.
- The Site Recovery Mobility service extension is automatically installed on the VM.
- The extension registers the VM with Site Recovery.
- Continuous replication begins for the VM. Disk writes are immediately transferred to the cache storage account in the source location.
- Site Recovery processes the data in the cache, and sends it to the target storage account, or to the replica managed disks.
- After the data is processed, crash-consistent recovery points are generated every five minutes.
- App-consistent recovery points are generated according to the setting specified in the replication policy.



Consistency

Crash-consistent

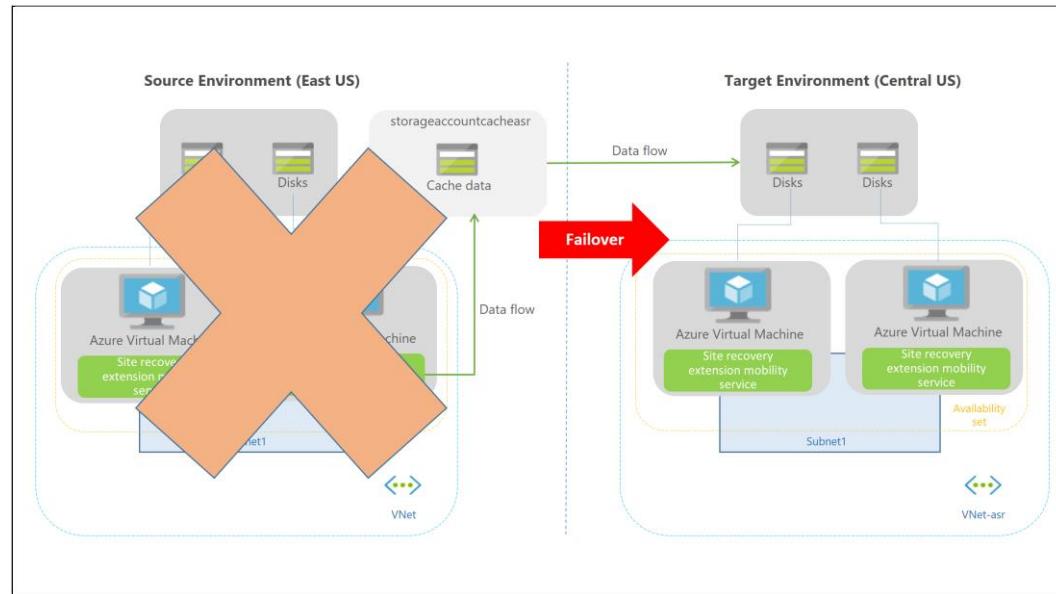
- Captures data that was on the disk when the snapshot was taken. It doesn't include anything in memory.
- Doesn't guarantee data consistency for the operating system, or for apps on the VM.

App-consistent

- App-consistent recovery points are created from app-consistent snapshots.
- contain all the information in a crash-consistent snapshot, plus all the data in memory and transactions in progress.

Failover process

- When you initiate a failover, the VMs are created in the target resource group, target virtual network, target subnet, and in the target availability set.
- During a failover, you can use any recovery point.



Azure Portal

One stop shop – Single portal, single login for all your Azure assets

Azure Portal

- Web-based user interface to almost all Azure features.
- See all your services, create new ones, configure them, and see reports
- Single login for all user assets

When Portal is preferred?

- Occasionally management and administrative tasks can be performed via the Azure portal.
- A visual interface for reporting makes sense if you're just learning Azure and only need to set up and manage resources occasionally.

When Portal is not preferred?

- The routine setup, teardown, and maintenance of a single resource or multiple connected resources.
- Use scripts - Powershell or CLI

```
$AppRule1 = New-AzFirewallApplicationRule -Name Allow-Google -SourceAddress 10.0.2.0/24  
-Protocol http, https -TargetFqdn www.google.com  
  
$AppRuleCollection = New-AzFirewallApplicationRuleCollection -Name App-Coll01  
-Priority 200 -ActionType Allow -Rule $AppRule1  
  
$Azfw.ApplicationRuleCollections.Add($AppRuleCollection)  
  
Set-AzFirewall -AzureFirewall $Azfw
```

PowerShell

- PowerShell can be used to manage tasks from the command line and automate tasks across multiple platforms.
 - Cross-platform task automation scripting language
- Initially designed for system administrators
 - Can perform every possible management task
 - Windows PowerShell, which was previously a Windows-only component, became open-source and cross-platform on August 18, 2016, with the release of PowerShell Core.
- PowerShell accepts and returns .NET objects. (Unlike most shells that only accept and return text)
- Extensible through modules
- Deploy and Manage almost any technology:
 - Runs on Windows, Linux, and macOS
 - Microsoft: Azure, Windows, Exchange, SQL etc.
 - Third-party: AWS, VMWare, Google Cloud etc.
- Exam Perspective:
 - You don't have to write scripts
 - Code will be given either in question or options, you have to select the right one

Cmdlet (PowerShell Command)

- Commands for PowerShell are known as cmdlets (pronounced command-lets)
- Cmdlets can be executed independently or combined into a script file
- PowerShell uses a Verb-Noun name pair to name cmdlets.
 - Verb identifies the action that the cmdlet performs
 - Noun identifies the resource on which the cmdlet performs its action
 - Examples:
 - Get-Command -> retrieves a list of all commands installed on your machine.
 - Set-Date
 - Sort-Object
 - Start-Process
 - Stop-AzureVM
 - Write-Error
 - Get-Verb command to list all verbs
- Cmdlets are collected into PowerShell modules
 - Modules can be loaded on demand
 - Get-Module –ListAvailable command to list all modules

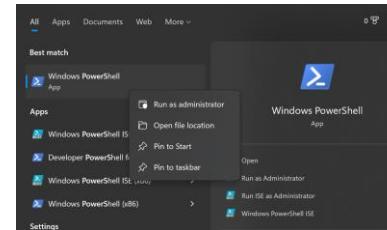
Azure PowerShell

- Azure PowerShell is a set of cmdlets for managing Azure resources directly from PowerShell.
- Azure PowerShell is available on Linux, macOS or Windows platforms.
- Common Scenarios: Day to day operations:
 - Automation of repetitive tasks
 - Scheduling
 - Deployments
 - Routine setup, teardown, and maintenance of a single resource or multiple connected resources.
- Two Module:
 - AzureRM (Azure Resource Management - old)
 - Az -> (Renamed, new, recommended)
- **Az** PowerShell module is a wrapper module
 - Az.Network for Azure networking services
 - Az.AKS for Azure Kubernetes Service.

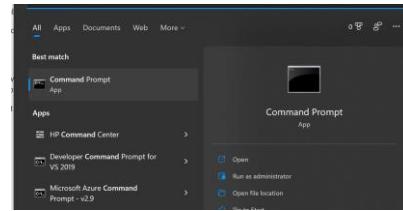
PowerShell vs CLI

PowerShell vs CLI

- Primary difference is the syntax
- Windows administrators can prefer PowerShell.
- Linux administrators can prefer Azure CLI, similar to Bash scripting.



PowerShell



CLI

Command	Azure CLI	Azure PowerShell
Sign in with Web Browser	az login	Connect-AzAccount
Get available subscriptions	az account list	Get-AzSubscription
Set Subscription	az account set --subscription <SubscriptionId>	Set-AzContext -Subscription <SubscriptionID>
List Azure Locations	az account list-locations	Get-AzLocation

PowerShell vs CLI

PowerShell	CLI
➤ Get-AzVM	➤ az vm create
➤ New-AzVM	➤ az vm list
➤ Remove-AzVM	➤ az resize
➤ Get-AzSqlDatabase	➤ az sql db copy
➤ New-AzSqlDatabase	➤ az sql db create
➤ Remove-AzSqlServer	➤ az sql db delete
➤ Get-AzVirtualNetwork	➤ az network vnet create
➤ New-AzVirtualNetwork	➤ az network vnet delete
➤ Remove-AzVirtualNetwork	➤ az network vnet list
➤ Set-AzVirtualNetworkPeering	➤ az network vnet peering create
➤ Get-AzVirtualNetworkPeering	➤ az network vnet peering delete
➤ Remove-AzVirtualNetworkPeering	➤ az network vnet peering list

Command-Line Interface (CLI)

- Azure Command-Line Interface (CLI) is a cross-platform command-line tool to manage Azure resources.
- You can install the Azure CLI locally on Linux, Mac, or Windows computers.
 - Or use from Azure Cloud Shell Or run from inside a Docker container.

Different shell environments

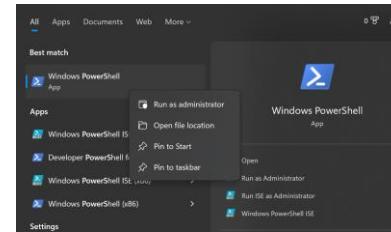
Shell Environment	Azure CLI	Azure PowerShell
Cmd	Yes	
Bash	Yes	
Windows PowerShell	Yes	Yes
PowerShell	Yes	Yes

Azure PowerShell

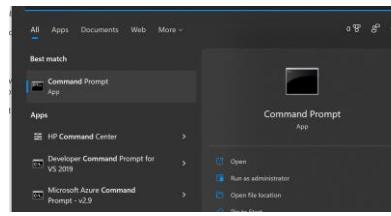
command-line tools that enable you to create and manage Azure resources.

PowerShell vs CLI vs Cloud Shell

- PowerShell can execute commands called Cmdlets
- Commands call the Azure Rest API
- Can perform every possible management task in Azure
- Cmdlets can be executed independently or combined into a script file
 - Script makes the process repeatable and automatable
- The routine setup, teardown, and maintenance of a single resource or multiple connected resources.
- Available for Windows, Linux, and Mac
- PowerShell can work with other platform as well



PowerShell



CLI

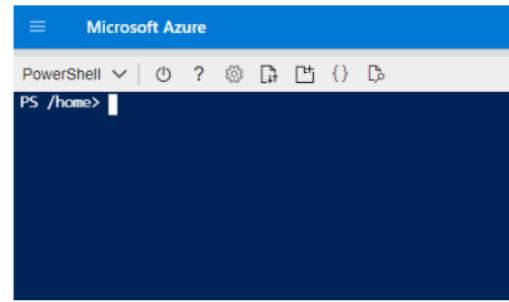
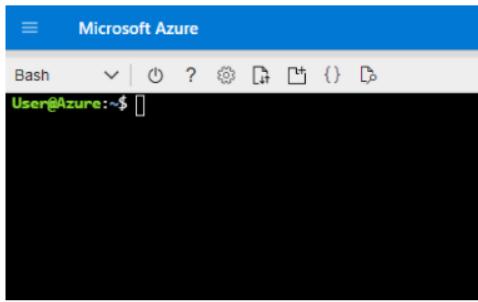
PowerShell vs CLI

- Primary difference is the syntax
- Windows administrators can prefer PowerShell.
- Linux administrators can prefer Azure CLI, similar to Bash scripting.

Command	Azure CLI	Azure PowerShell
Sign in with Web Browser	az login	Connect-AzAccount
Get available subscriptions	az account list	Get-AzSubscription
Set Subscription	az account set --subscription <SubscriptionId>	Set-AzContext -Subscription <SubscriptionID>
List Azure Locations	az account list-locations	Get-AzLocation

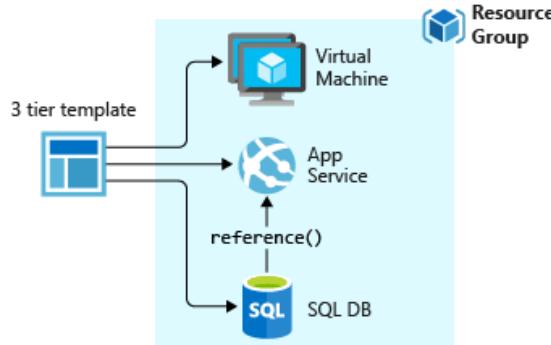
Azure Cloud Shell

- An interactive shell that runs in the browser for free (Access from Azure Portal)
- Pre-installed and configured Azure tools like interpreters or modules.
- Language support for Node.js, .Net and python
- Supports both PowerShell and CLI (bash)
- Dedicated storage to persist between sessions
- Integrated file editor



When PowerShell or CLI are not preferred?

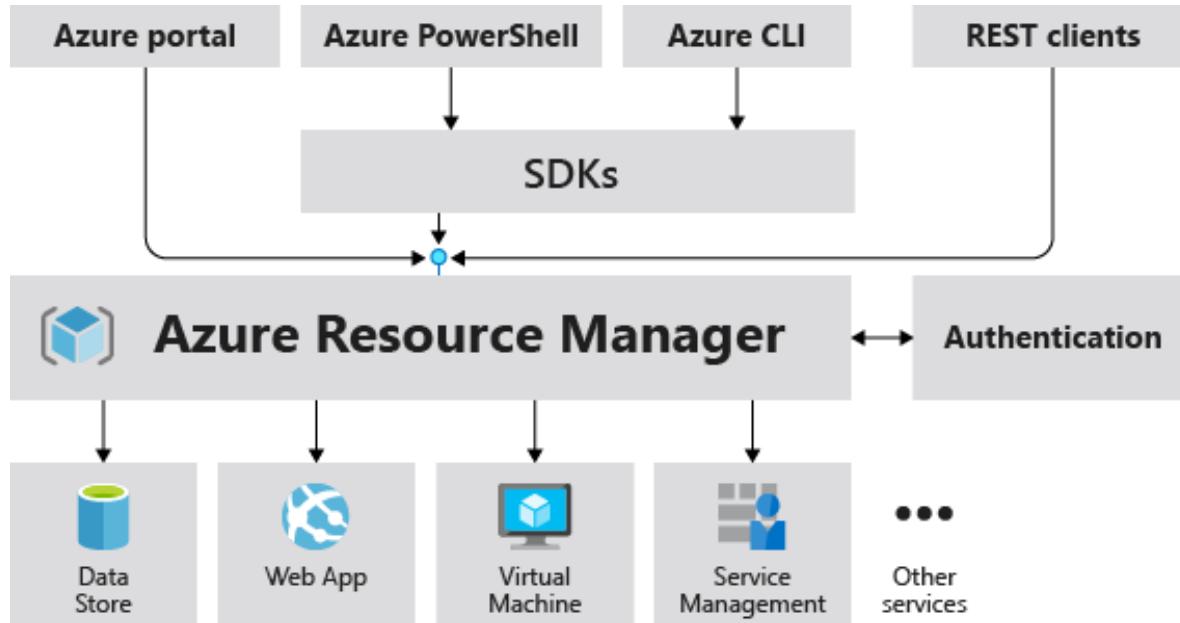
- The deployment of an entire infrastructure, which might contain dozens or hundreds of resources, from imperative code.
- A validation step ensures that all resources can be created in the proper order based on dependencies, **in parallel**, and idempotent.
- ARM template – Azure Resource Manager



Azure Resource Manager (ARM)

Deployment and management service for Azure

Azure Resource Manager



Azure Resource Manager

- Deployment and management service for Azure
- All Azure resource activities are routed via ARM.
- Describe the resources in a declarative JSON format
- ARM template is verified before any code is executed to ensure that the resources will be created and connected correctly
- Automatic Rollback in case of failure
- The template then orchestrates the creation of those resources in parallel
- Templates can even execute PowerShell and Bash scripts before or after the resource has been set up
- Creates all dependencies in the correct order
- Save previous scripts for version control
- ARM templates define your application's infrastructure requirements for a repeatable deployment that is done in a consistent manner
- Why not PowerShell or CLI?
 - No validation step in these tools
 - If a script encounters an error, the dependency resources can't be rolled back easily
 - Deployments happen serially
 - You have to figure out dependencies

