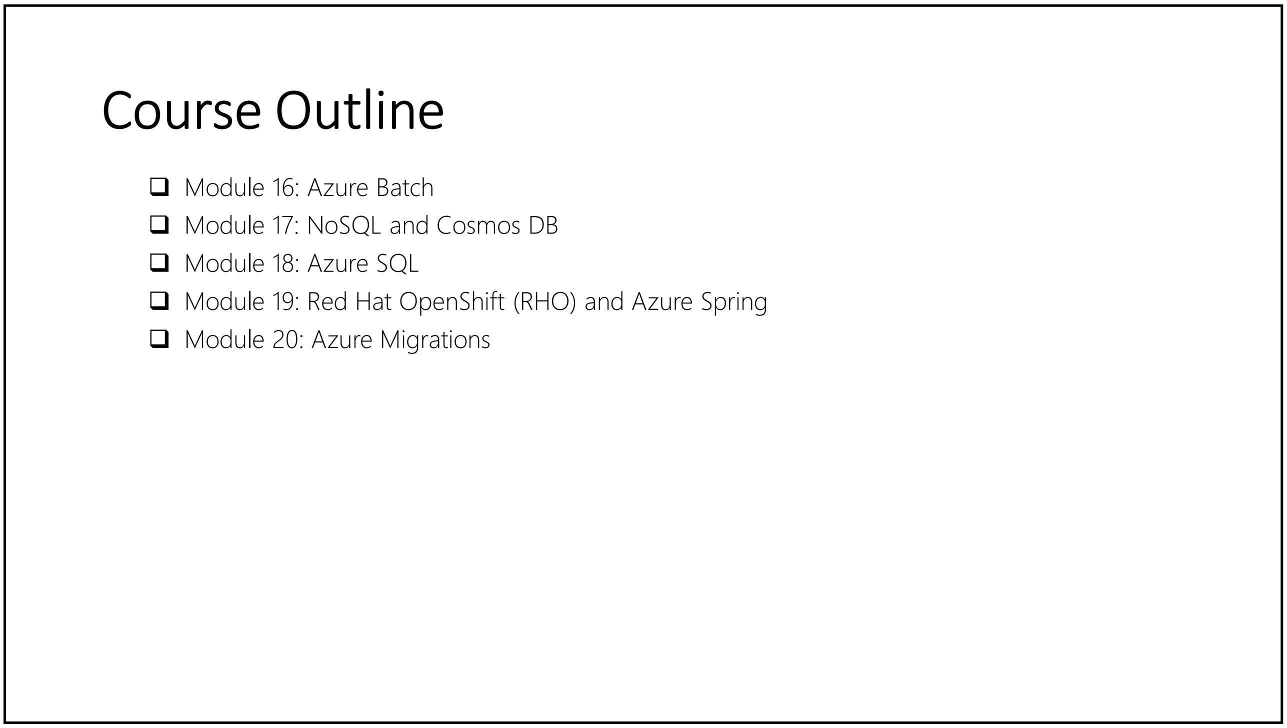
Microsoft Certified: Azure Solutions Architect Expert: AZ-305

Kevin Brown
MCT (Microsoft Certified Trainer) since 2000
Azure Security Engineer, Azure Solutions Architect, Azure Administrator
Microsoft 365 Enterprise Administrator, Microsoft 365 Security Administrator
MCSA, CISSP, CCIE: Routing and Switching

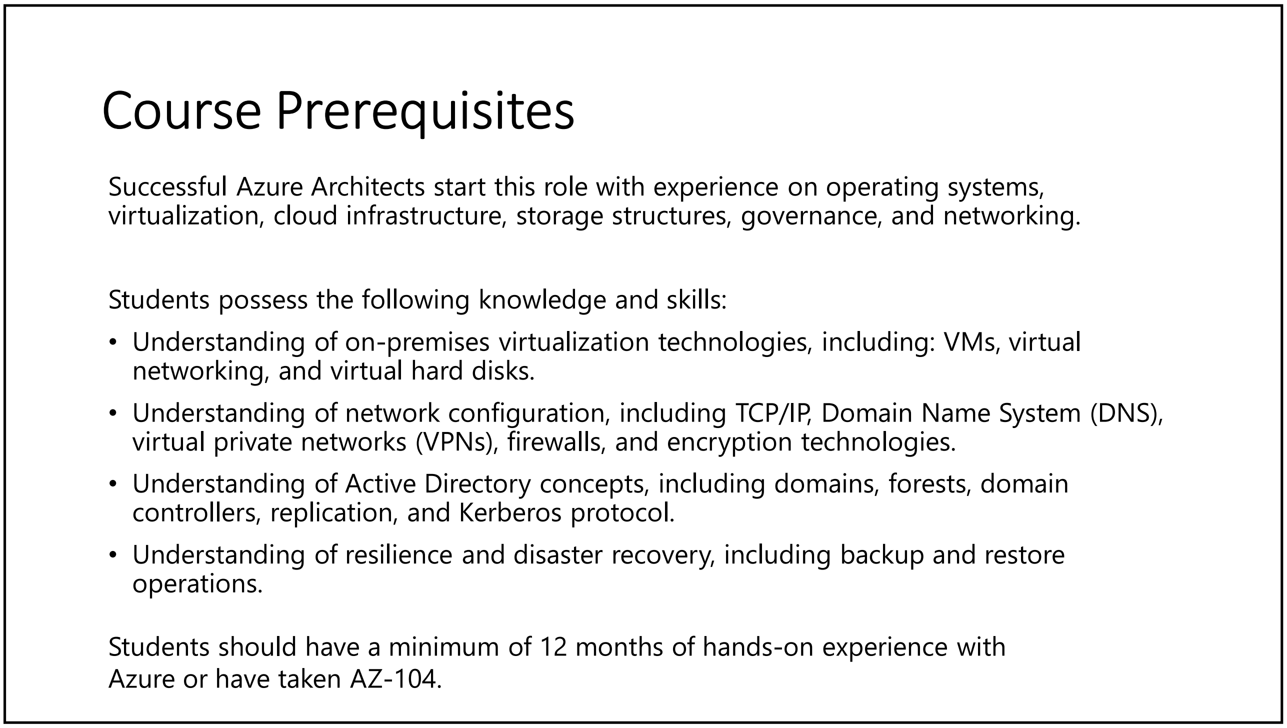
Course Outline

- Module 1: Planning and Assessments
- Module 2: Azure Virtual Networking
- Module 3: Azure Virtual Machines
- Module 4: Azure Templates
- Module 5: Azure Load Balancer
- Module 6: Azure Storage
- Module 7: Identity Management
- Module 8: Azure Roles
- Module 9: Azure Sentinel
- Module 10: Planning Azure AD Connect and Azure AD Cloud Sync
- Module 11: Planning and Managing Azure Backups
- Module 12: Monitoring Azure Resources and Services
- Module 13: Azure Key Vault
- Module 14: Azure Applications
- Module 15: Azure Containers and Kubernetes



Course Outline

- ❑ Module 16: Azure Batch
- ❑ Module 17: NoSQL and Cosmos DB
- ❑ Module 18: Azure SQL
- ❑ Module 19: Red Hat OpenShift (RHO) and Azure Spring
- ❑ Module 20: Azure Migrations



Course Prerequisites

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

Students possess the following knowledge and skills:

- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of Active Directory concepts, including domains, forests, domain controllers, replication, and Kerberos protocol.
- Understanding of resilience and disaster recovery, including backup and restore operations.

Students should have a minimum of 12 months of hands-on experience with Azure or have taken AZ-104.

Module 1:

Assessing the current environment

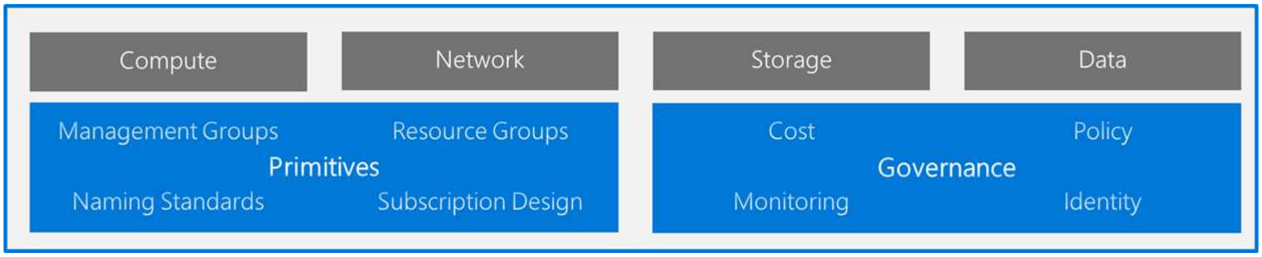
Topics Covered

❑Understanding Landing Zones

❑Azure Assessments

Understanding Landing Zones

A landing zone is the basic building block of any cloud adoption environment. The term ***landing zone*** refers to an environment that's been provisioned and prepared to host workloads in a cloud environment like Azure. A fully functioning landing zone is the final deliverable of any iteration of the Cloud Adoption.



Compute

Network

Storage

Data

Management Groups

Resource Groups

Primitives

Naming Standards

Subscription Design

Cost

Policy

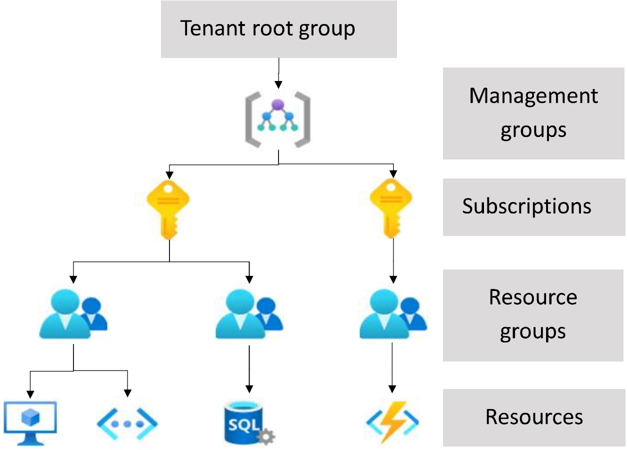
Governance

Monitoring

Identity

Govern resources in Azure

- Governance is the process to maintain control over your applications and resources in Azure
- Governance involves determining your requirements, planning your initiatives, and settings strategic principles



Tenant root group

Management groups

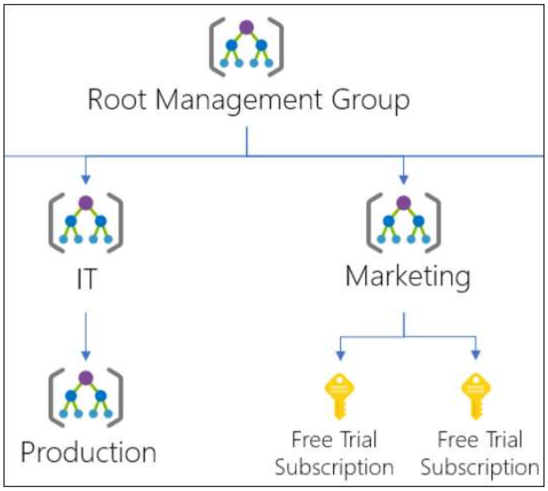
Subscriptions

Resource groups

Resources

Planning for management groups

- Keep the management group hierarchy reasonably flat
- Consider a top-level management group
- Consider an organizational or departmental structure
- Consider a geographical structure
- Consider a production management group
- Consider a sandbox management group
- Consider isolating sensitive information in a separate management group

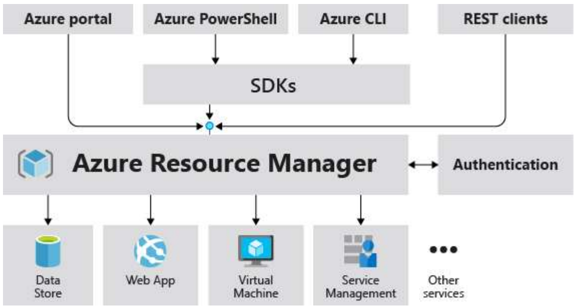


Designing for multiple subscriptions

- Align your subscriptions with business needs and priorities – consider billing and cost reporting
- Consider administrative management – centralized or decentralized
- Group subscriptions together under management groups – apply common policies and role assignments.
- Consider subscription scale limits – specialized workloads, IoT, SAP
- Consider a dedicated shared services subscription – common services everyone shares
- Make subscription owners aware of their roles and responsibilities

**Important: Networking, does not span subscriptions without special configuration. This is a specific example of how subscriptions can help with isolation and management.

Planning resource groups



- Group resources that share the same life cycle
- Group by type, app, department, location, or billing
- Apply RBAC and policies to a group of resources
- Use resource locks to protect individual resources from deletion or change

The benefits of using Resource Manager

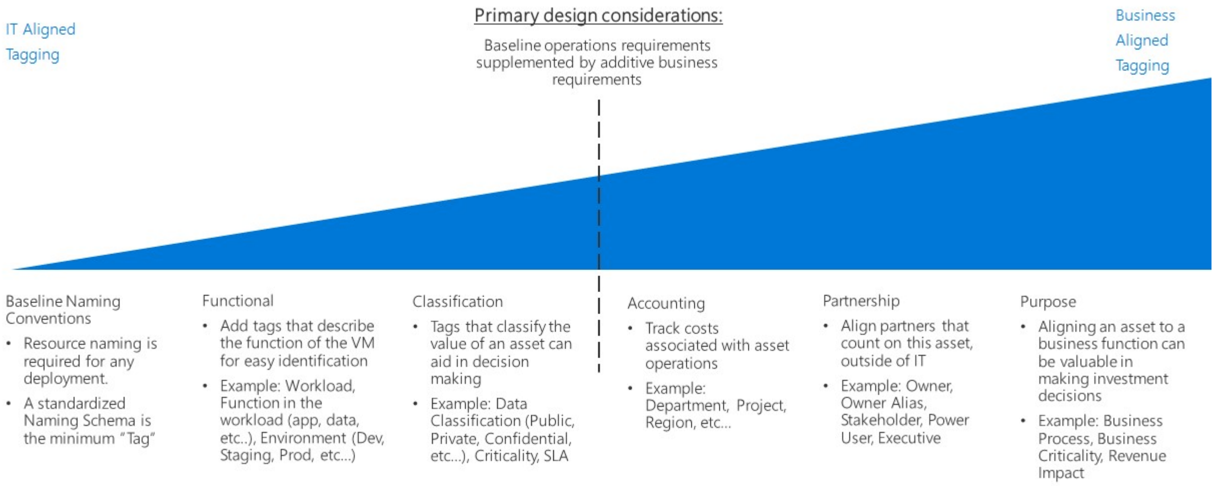
- Manage your infrastructure through declarative templates rather than scripts.
- Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.
- Redeploy your solution throughout the development lifecycle and have confidence your resources are deployed in a consistent state.
- Define the dependencies between resources so they're deployed in the correct order.
- Apply access control to all services because Azure role-based access control (Azure RBAC) is natively integrated into the management platform.

Planning resource tagging

Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Use naming and tagging standards to organize your resources for the following reasons:

- **Resource management**
- **Cost management**
- **Operations management**
- **Security**
- **Governance and regulatory compliance**

Planning resource tagging



IT Aligned Tagging

Primary design considerations:

Baseline operations requirements supplemented by additive business requirements

Business Aligned Tagging

Baseline Naming Conventions

- Resource naming is required for any deployment.
- A standardized Naming Schema is the minimum "Tag"

Functional

- Add tags that describe the function of the VM for easy identification
- Example: Workload, Function in the workload (app, data, etc..), Environment (Dev, Staging, Prod, etc...)

Classification

- Tags that classify the value of an asset can aid in decision making
- Example: Data Classification (Public, Private, Confidential, etc...), Criticality, SLA

Accounting

- Track costs associated with asset operations
- Example: Department, Project, Region, etc...

Partnership

- Align partners that count on this asset, outside of IT
- Example: Owner, Owner Alias, Stakeholder, Power User, Executive

Purpose

- Aligning an asset to a business function can be valuable in making investment decisions
- Example: Business Process, Business Criticality, Revenue Impact

Planning resource tagging

The following example applies a set of tags to a storage account:

```
$tags = @{"Dept"="Finance"; "Status"="Normal"}
$resource = Get-AzResource -Name demoStorage -ResourceGroup demoGroup
New-AzTag -ResourceId $resource.id -Tag $tags
```

To get resources that have a specific tag name and value, use:

```
(Get-AzResource -Tag @{ "CallCenter"=“Brazil02"}).Name
```

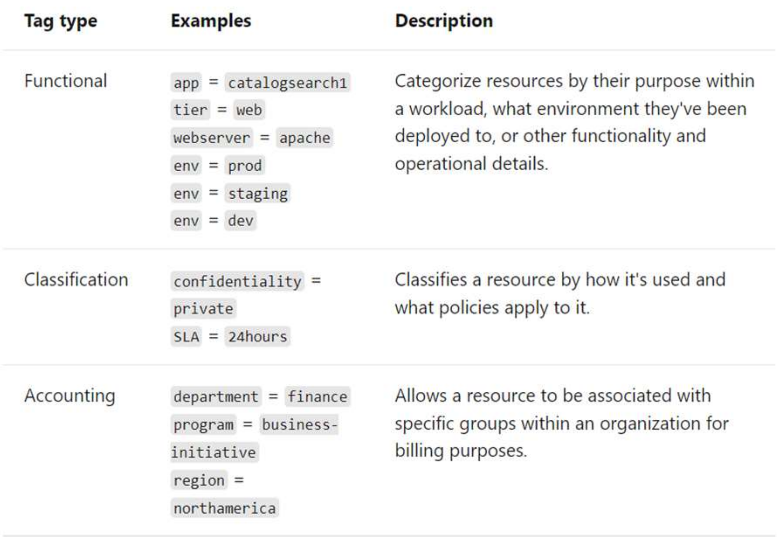
To get resources that have a specific tag name with any tag value, use:

```
(Get-AzResource -TagName “SalesDept").Name
```

To get resource groups that have a specific tag name and value, use:

```
(Get-AzResourceGroup -Tag @{ "CallCenter"=“Brazil02" }).ResourceGroupName
```

Planning resource tagging



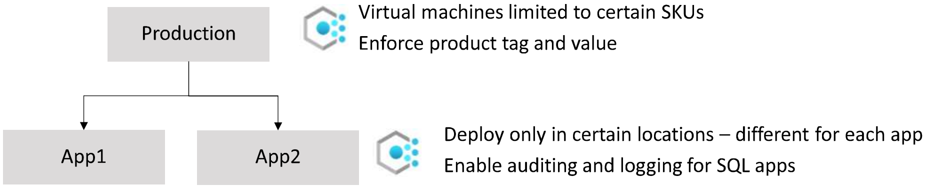
Tag type	Examples	Description

Functional	`app` = `catalogsearch1`
	`tier` = `web`
	`webserver` = `apache`
	`env` = `prod`
	`env` = `staging`
	`env` = `dev`
		Categorize resources by their purpose within a workload, what environment they've been deployed to, or other functionality and operational details.

Classification	`confidentiality` = `private`
	`SLA` = `24hours`
		Classifies a resource by how it's used and what policies apply to it.

Accounting	`department` = `finance`
	`program` = `business-initiative`
	`region` = `northamerica`
		Allows a resource to be associated with specific groups within an organization for billing purposes.

Using Azure Policy

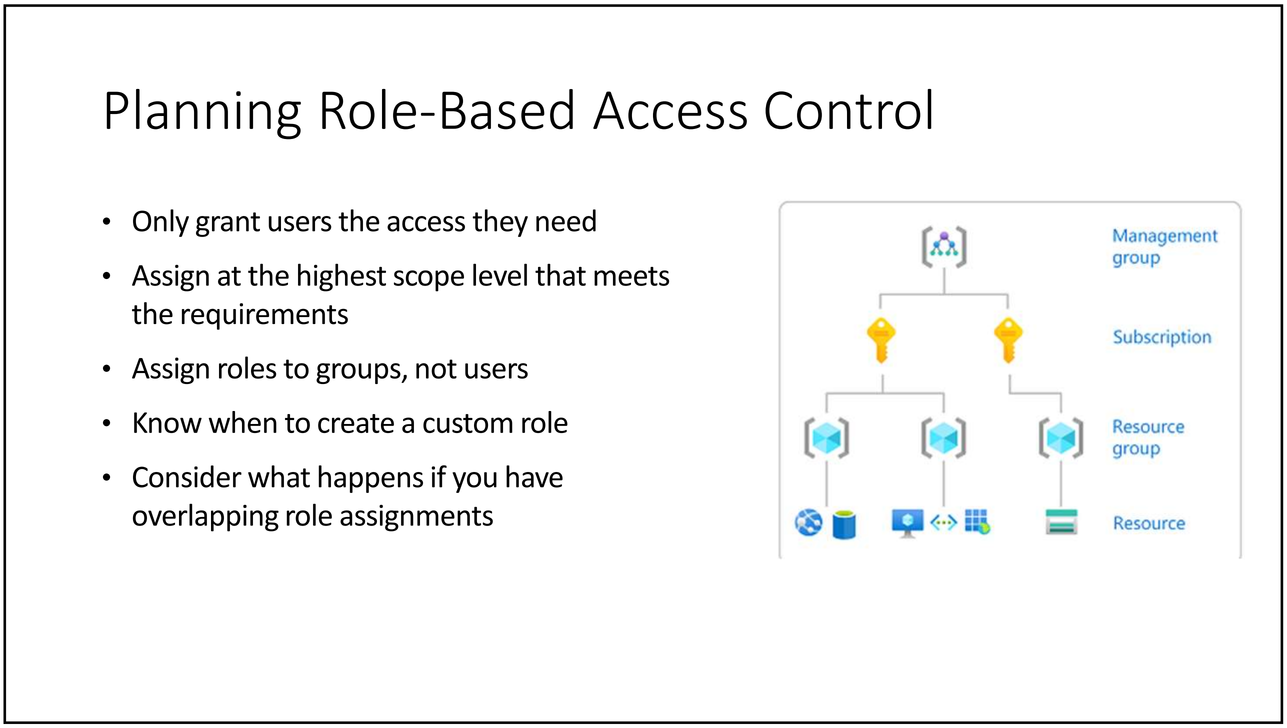


Production
Virtual machines limited to certain SKUs
Enforce product tag and value
App1
App2
Deploy only in certain locations – different for each app
Enable auditing and logging for SQL apps

- Azure Policy helps to enforce organizational standards and to assess compliance at-scale.
- Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

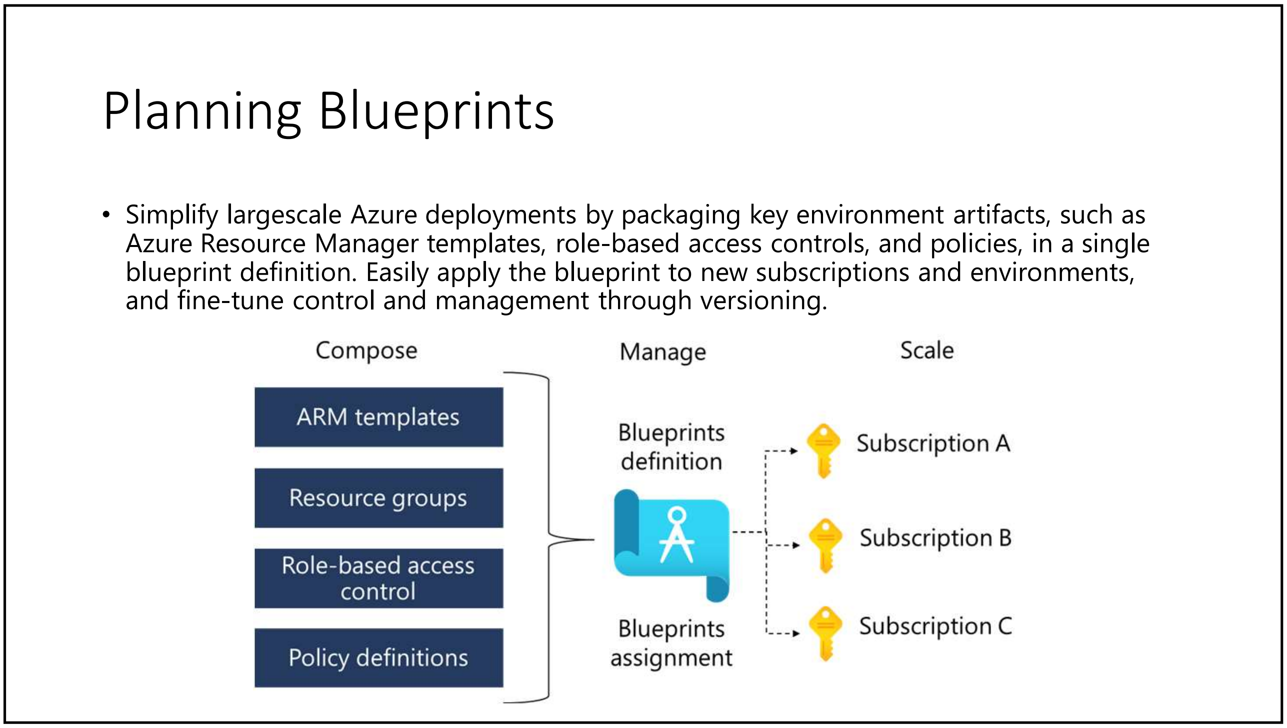
Recommendations for Azure Policy deployment

- Apply policy at the highest scope possible
- Decide what to do if a resource is non-compliant
- Consider when to automatically remediate non-compliant resources
- Use the Azure policy compliance dashboard for auditing and review



Planning Role-Based Access Control

- Only grant users the access they need
- Assign at the highest scope level that meets the requirements
- Assign roles to groups, not users
- Know when to create a custom role
- Consider what happens if you have overlapping role assignments



Planning Blueprints

- Simplify largescale Azure deployments by packaging key environment artifacts, such as Azure Resource Manager templates, role-based access controls, and policies, in a single blueprint definition. Easily apply the blueprint to new subscriptions and environments, and fine-tune control and management through versioning.

Compose

ARM templates

Resource groups

Role-based access control

Policy definitions

Manage

Blueprints definition

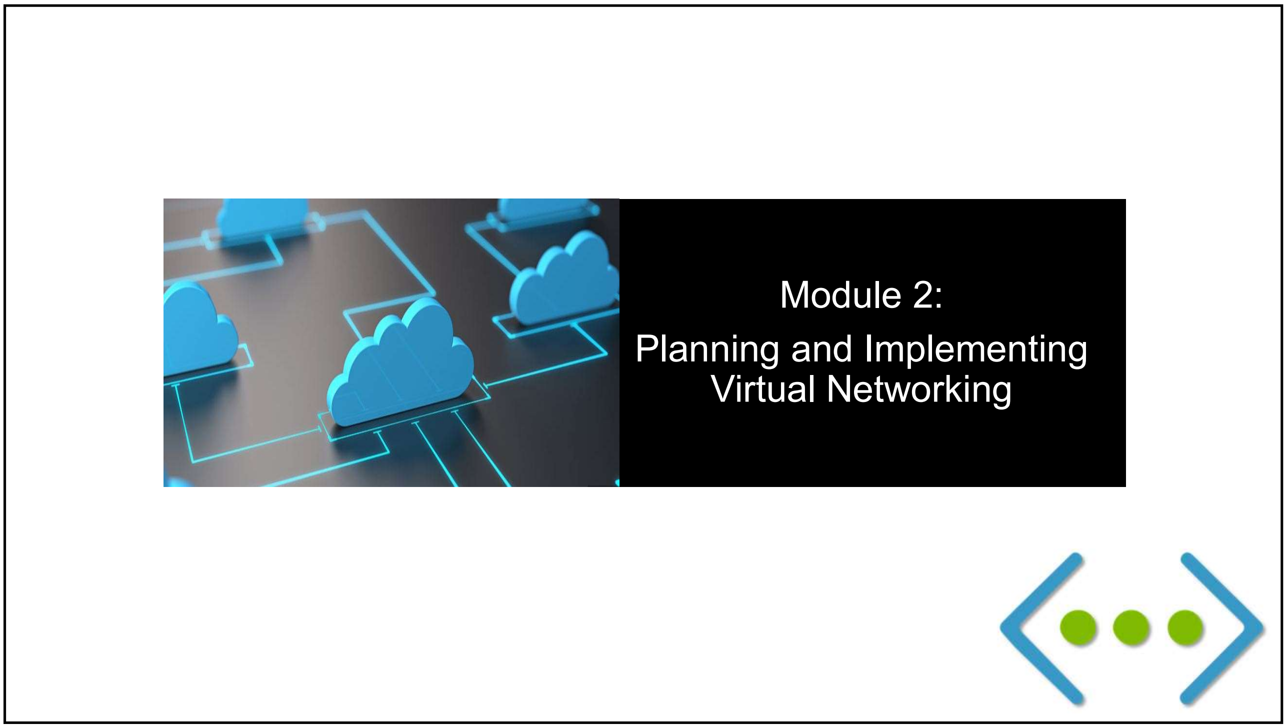
Blueprints assignment

Scale

Subscription A

Subscription B

Subscription C

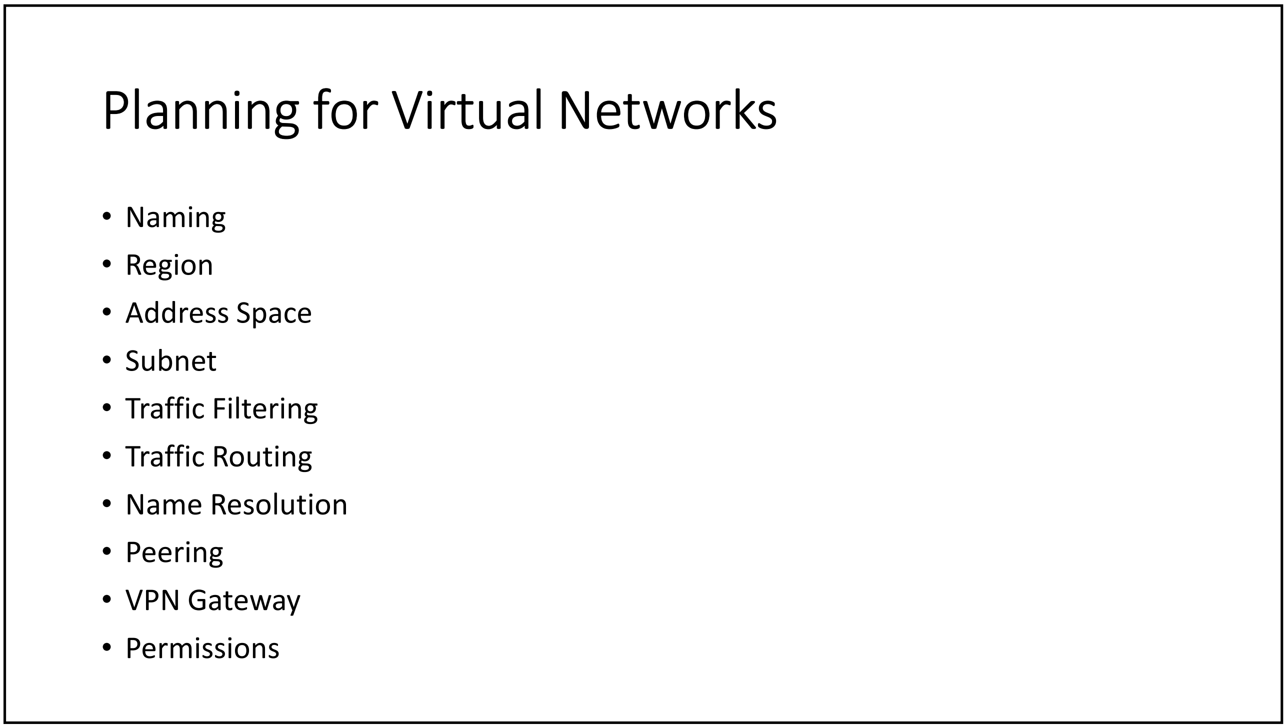


Module 2:

Planning and Implementing Virtual Networking

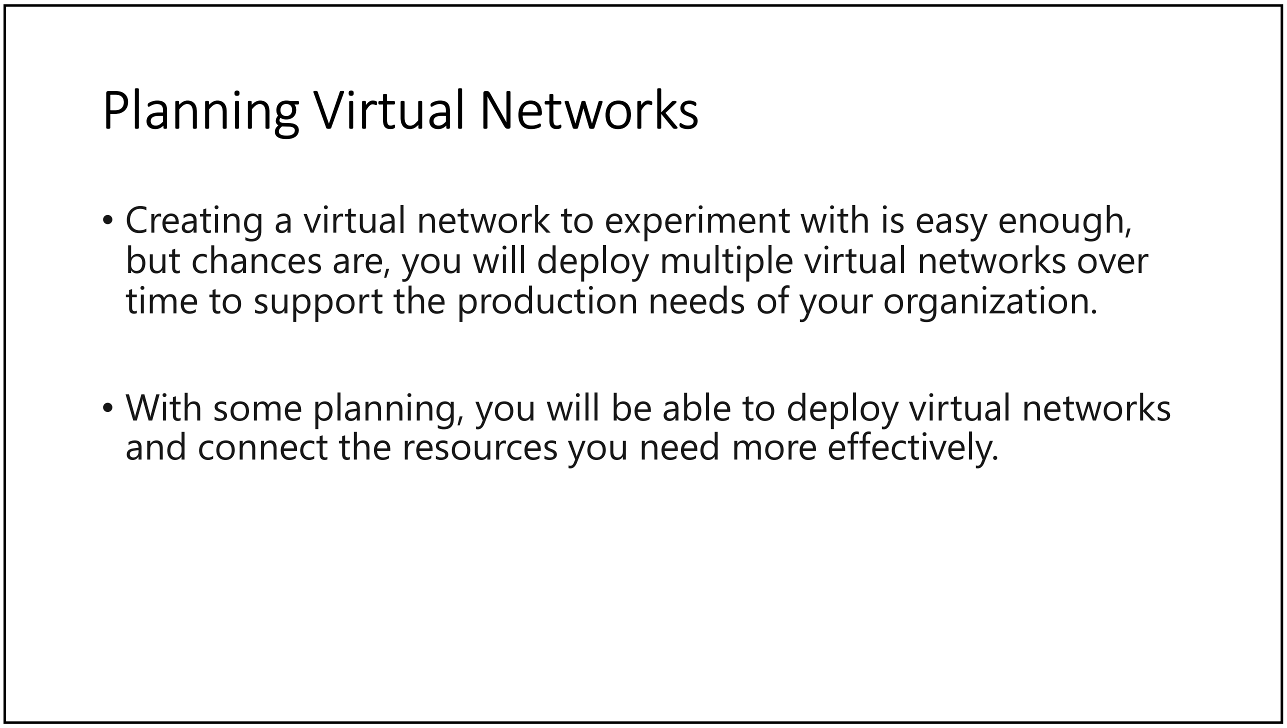
Topics Covered

- ❑Understanding virtual networking
- ❑Planning for network connectivity
- ❑VPN gateway
- ❑Application gateway
- ❑Vnet peering
- ❑Traffic routing
- ❑Gateway transit
- ❑Express routes
- ❑Filtering network traffic



Planning for Virtual Networks

- Naming
- Region
- Address Space
- Subnet
- Traffic Filtering
- Traffic Routing
- Name Resolution
- Peering
- VPN Gateway
- Permissions



Planning Virtual Networks

- Creating a virtual network to experiment with is easy enough, but chances are, you will deploy multiple virtual networks over time to support the production needs of your organization.

- With some planning, you will be able to deploy virtual networks and connect the resources you need more effectively.

Naming

- All Azure resources have a name. The name must be unique within a scope, that may vary for each resource type. For example, the name of a virtual network must be unique within a resource group, but can be duplicated within a subscription or Azure region. Defining a naming convention that you can use consistently when naming resources is helpful when managing several network resources over time.

Regions

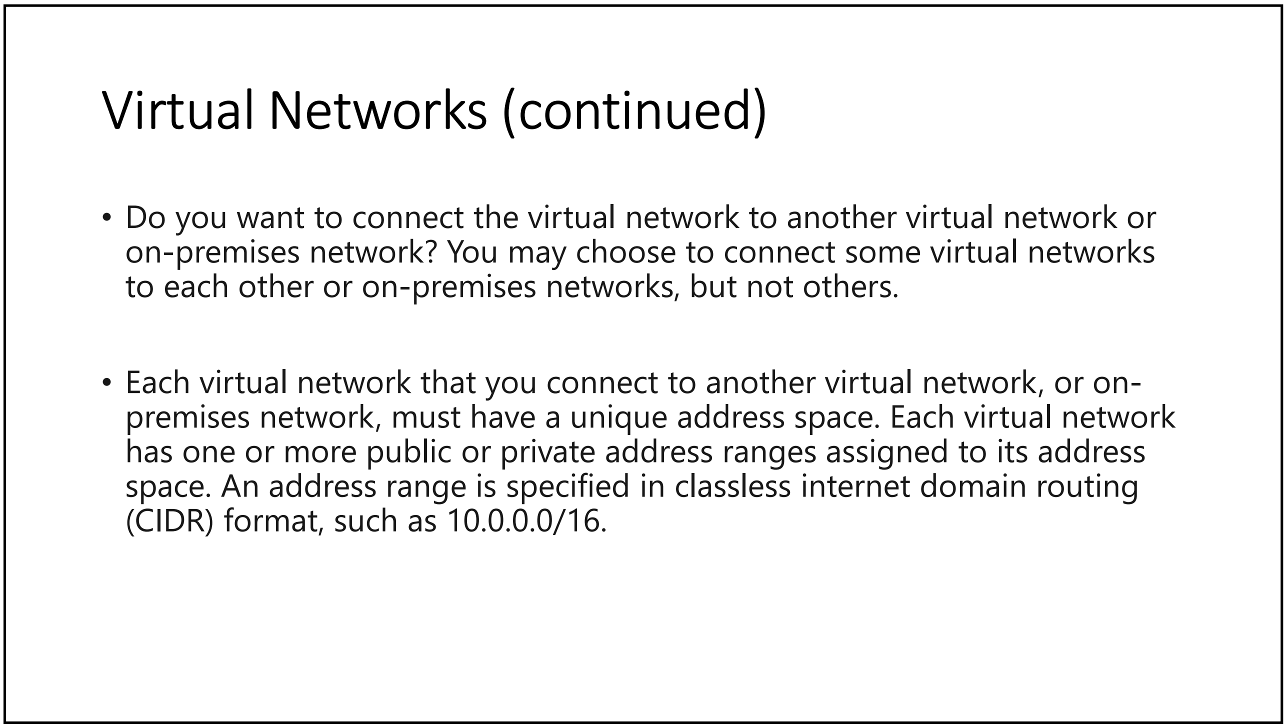
- All Azure resources are created in an Azure region and subscription. A resource can only be created in a virtual network that exists in the same region and subscription as the resource. You can however, connect virtual networks that exist in different subscriptions and regions.
- Do you have data residency, sovereignty, compliance, or resiliency requirements? If so, choosing the region that aligns to the requirements is critical.
- Do you require resiliency across Azure Availability Zones within the same Azure region for the resources you deploy? You can deploy resources, such as virtual machines (VM) to different availability zones within the same virtual network. Not all Azure regions support availability zones however.

Segmentation

- You can create multiple virtual networks per subscription and per region. You can create multiple subnets within each virtual network. The considerations that follow help you determine how many virtual networks and subnets you require:

Virtual Networks

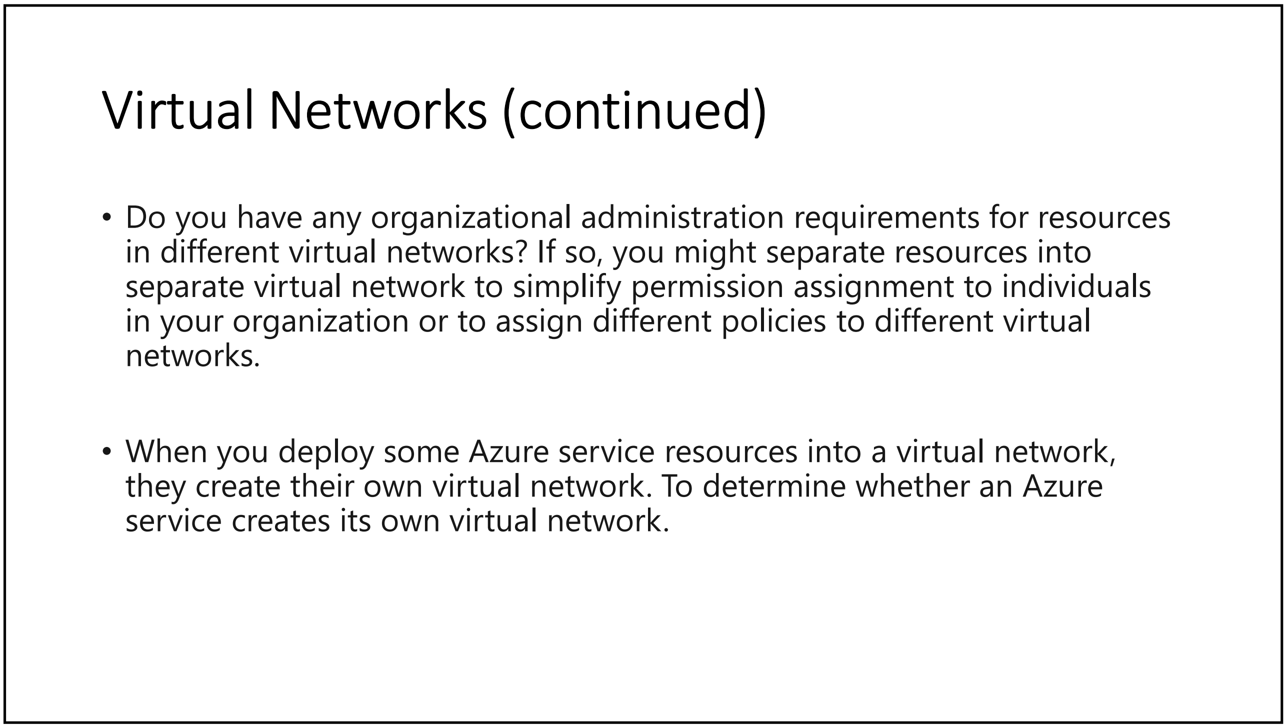
- A virtual network is a virtual, isolated portion of the Azure public network. Each virtual network is dedicated to your subscription. Things to consider when deciding whether to create one virtual network, or multiple virtual networks in a subscription:
- Do any organizational security requirements exist for isolating traffic into separate virtual networks? You can choose to connect virtual networks or not. If you connect virtual networks, you can implement a network virtual appliance, such as a firewall, to control the flow of traffic between the virtual networks.
- Do any organizational requirements exist for isolating virtual networks into separate subscriptions or regions?



Virtual Networks (continued)

- Do you want to connect the virtual network to another virtual network or on-premises network? You may choose to connect some virtual networks to each other or on-premises networks, but not others.

- Each virtual network that you connect to another virtual network, or on-premises network, must have a unique address space. Each virtual network has one or more public or private address ranges assigned to its address space. An address range is specified in classless internet domain routing (CIDR) format, such as 10.0.0.0/16.



Virtual Networks (continued)

- Do you have any organizational administration requirements for resources in different virtual networks? If so, you might separate resources into separate virtual network to simplify permission assignment to individuals in your organization or to assign different policies to different virtual networks.

- When you deploy some Azure service resources into a virtual network, they create their own virtual network. To determine whether an Azure service creates its own virtual network.

Subnets

- A virtual network can be segmented into one or more subnets. Things to consider when deciding whether to create one subnet, or multiple virtual networks in a subscription:
- Each subnet must have a unique address range, specified in CIDR format, within the address space of the virtual network. The address range cannot overlap with other subnets in the virtual network.
- If you plan to deploy some Azure service resources into a virtual network, they may require, or create, their own subnet, so there must be enough unallocated space for them to do so. For example, if you connect a virtual network to an on-premises network using an Azure VPN Gateway, the virtual network must have a dedicated subnet for the gateway.

Subnets (continued)

- Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance, for example. If you require that traffic between resources in the same virtual network flow through a network virtual appliance (NVA), deploy the resources to different subnets.

- You can associate one network security group to each subnet in a virtual network. You can associate the same, or a different, network security group to each subnet. Each network security group contains rules, which allow or deny traffic to and from sources and destinations. Learn more about network security groups.

Traffic Filtering

- You can filter network traffic between resources in a virtual network using a network security group, an NVA that filters network traffic, or both. To deploy an NVA, such as a firewall, to filter network traffic, see the Azure Marketplace. When using an NVA, you also create custom routes to route traffic from subnets to the NVA.
- A network security group contains several default security rules that allow or deny traffic to or from resources. A network security group can be associated to a network interface, the subnet the network interface is in, or both. To simplify management of security rules, it's recommended that you associate a network security group to individual subnets, rather than individual network interfaces within the subnet, whenever possible.

Traffic Routing

- Azure creates several default routes for outbound traffic from a subnet. You can override Azure's default routing by creating a route table and associating it to a subnet. Common reasons for overriding Azure's default routing are:
  - Because you want traffic between subnets to flow through an NVA. To learn more about how to configure route tables to force traffic through an NVA.
  - Because you want to force all internet-bound traffic through an NVA, or on-premises, through an Azure VPN gateway. Forcing internet traffic on-premises for inspection and logging is often referred to as forced tunneling.

Name Resolution

- Resources in one virtual network cannot resolve the names of resources in a peered virtual network using Azure's built-in DNS. To resolve names in a peered virtual network, deploy your own DNS server, or use Azure DNS private domains. Resolving names between resources in a virtual network and on-premises networks also requires you to deploy your own DNS server.

Peering

- When using virtual network peering, the virtual networks can be in the same, or different, supported Azure regions. The virtual networks can be in the same or different Azure subscriptions (even subscriptions belonging to different Azure Active Directory tenants). Before creating a peering, it's recommended that you familiarize yourself with all of the peering requirements and constraints. Bandwidth between resources in virtual networks peered in the same region is the same as if the resources were in the same virtual network.

VPN Gateway

- You can use an Azure VPN Gateway to connect a virtual network to your on-premises network using a site-to-site VPN, or using a dedicated connection with Azure ExpressRoute.
- You can combine peering and a VPN gateway to create hub and spoke networks, where spoke virtual networks connect to a hub virtual network, and the hub connects to an on-premises network.

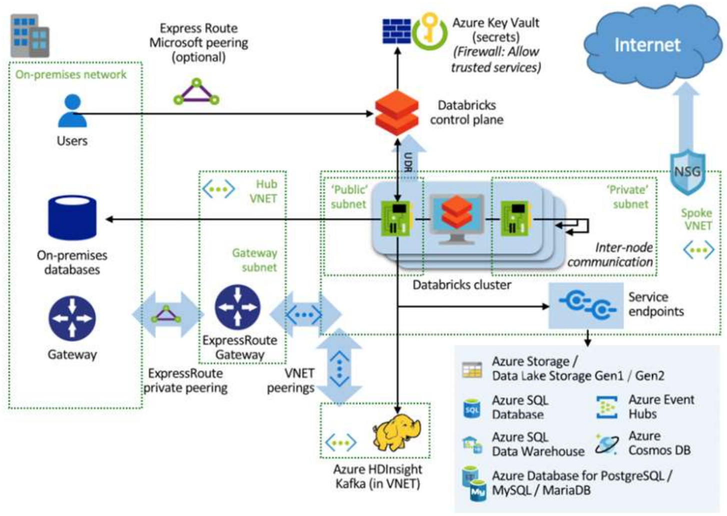
Permissions

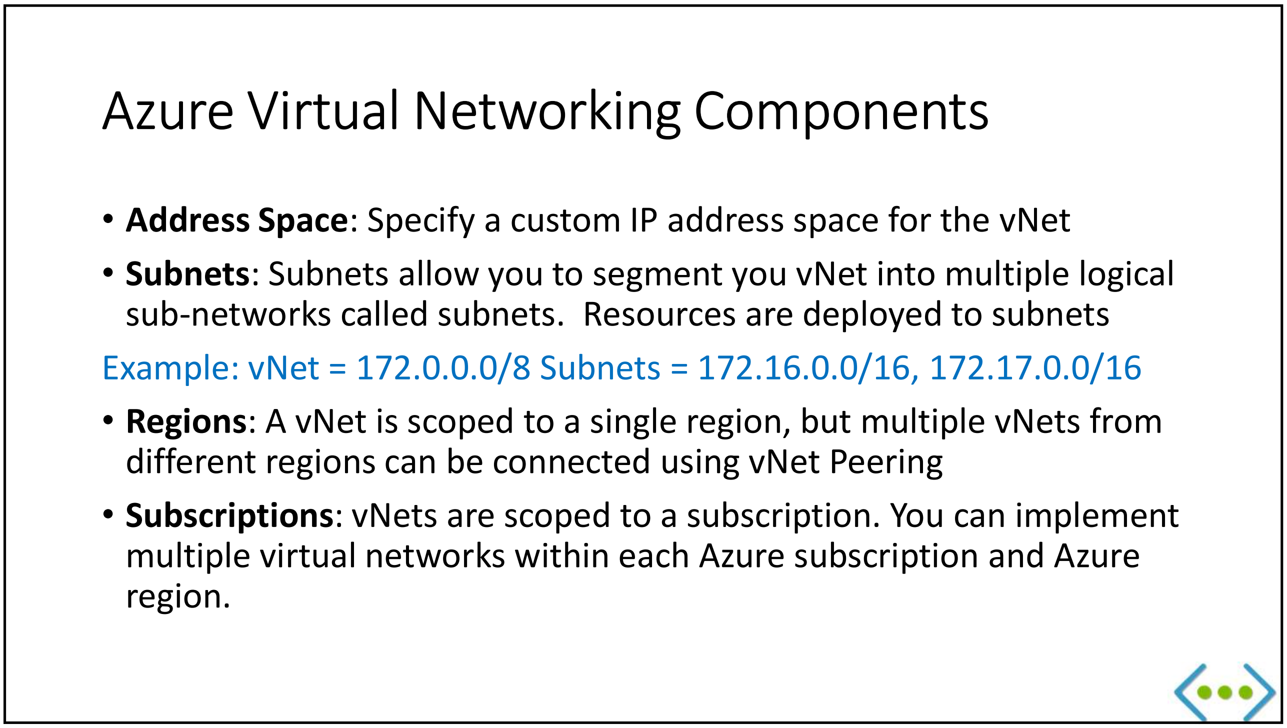
- Azure utilizes role based access control (RBAC) to resources. Permissions are assigned to a scope in the following hierarchy: management group, subscription, resource group, and individual resource.

Policy

- Azure Policy enables you to create, assign, and manage policy definitions. Policy definitions enforce different rules over your resources, so the resources stay compliant with your organizational standards and service level agreements. Azure Policy runs an evaluation of your resources, scanning for resources that are not compliant with the policy definitions you have.
- For example, you can define and apply a policy that allows creation of virtual networks in only a specific resource group or region. Another policy can require that every subnet has a network security group associated to it. The policies are then evaluated when creating and updating resources.

Understanding Virtual Networking (vNet)



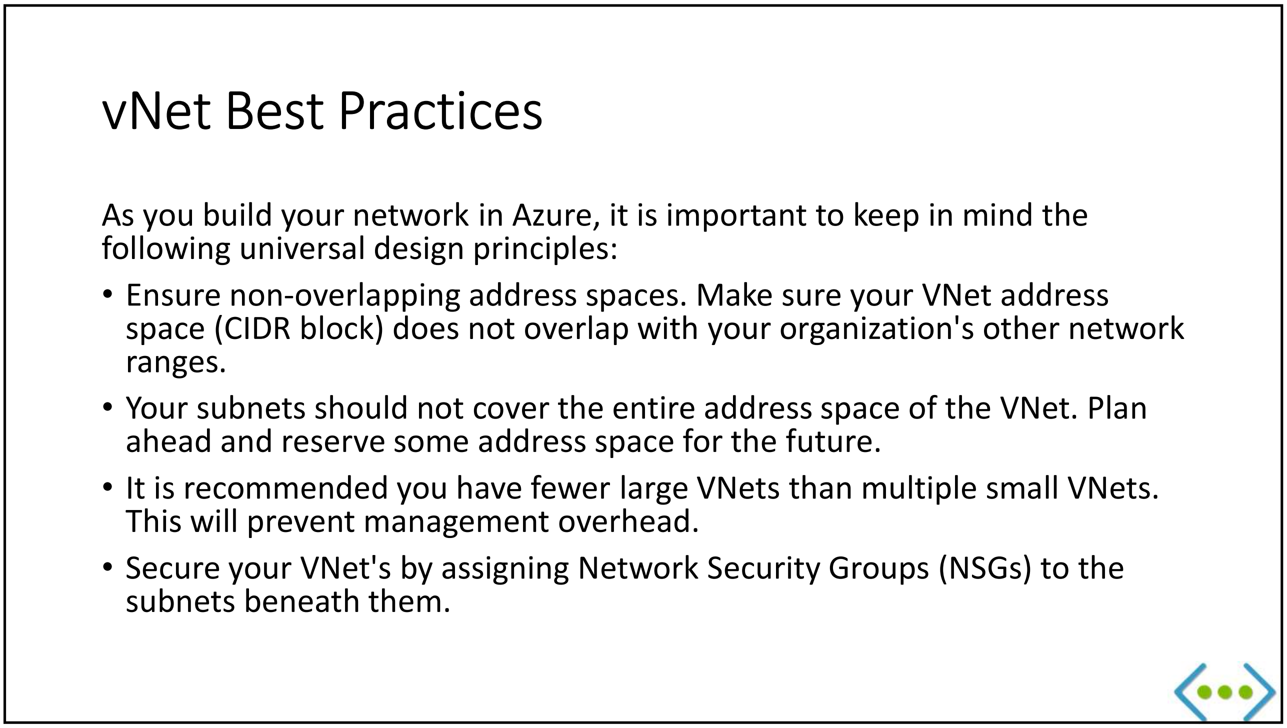


Azure Virtual Networking Components

- **Address Space**: Specify a custom IP address space for the vNet
- **Subnets**: Subnets allow you to segment you vNet into multiple logical sub-networks called subnets. Resources are deployed to subnets

Example: vNet = 172.0.0.0/8 Subnets = 172.16.0.0/16, 172.17.0.0/16

- **Regions**: A vNet is scoped to a single region, but multiple vNets from different regions can be connected using vNet Peering
- **Subscriptions**: vNets are scoped to a subscription. You can implement multiple virtual networks within each Azure subscription and Azure region.



vNet Best Practices

As you build your network in Azure, it is important to keep in mind the following universal design principles:

- Ensure non-overlapping address spaces. Make sure your VNet address space (CIDR block) does not overlap with your organization's other network ranges.
- Your subnets should not cover the entire address space of the VNet. Plan ahead and reserve some address space for the future.
- It is recommended you have fewer large VNets than multiple small VNets. This will prevent management overhead.
- Secure your VNet's by assigning Network Security Groups (NSGs) to the subnets beneath them.

Communicate with the internet

All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use public IP or public Load Balancer to manage your outbound connections.

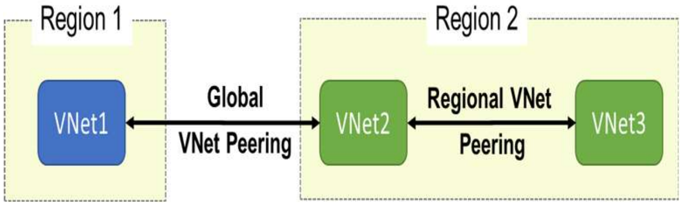
Communicate between Azure resources

- **Through a virtual network**: You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets.

- **Through a virtual network service endpoint**: Extend your virtual network private address space and the identity of your virtual network to Azure service resources, such as Azure Storage accounts and Azure SQL databases, over a direct connection. Service endpoints allow you to secure your critical Azure service resources to only a virtual network.

- **Through VNet Peering**: You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions.

VNet Peering



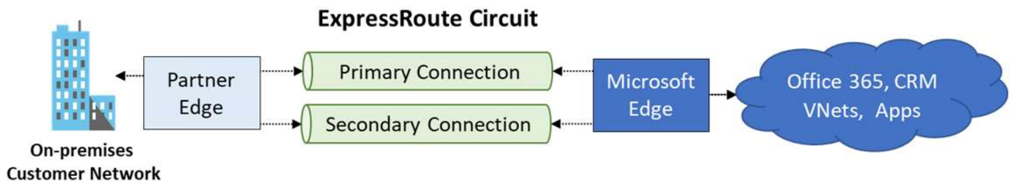
Communicate with on-premises resources

- **Point-to-site virtual private network (VPN)**: Established between a virtual network and a single computer in your network. Each computer that wants to establish connectivity with a virtual network must configure its connection. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The communication between your computer and a virtual network is sent through an encrypted tunnel over the internet.

- **Site-to-site VPN**: Established between your on-premises VPN device and an Azure VPN Gateway that is deployed in a virtual network. This connection type enables any on-premises resource that you authorize to access a virtual network. The communication between your on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet.

- **Azure ExpressRoute**: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.

ExpressRoute



ExpressRoute FAQ

If I pay for an ExpressRoute circuit of a given bandwidth, does the VPN connection I purchase from my network service provider have to be the same speed?

- No. You can purchase a VPN connection of any speed from your service provider. However, your connection to Azure is limited to the ExpressRoute circuit bandwidth that you purchase.

If I pay for an ExpressRoute circuit of a given bandwidth, do I have the ability to burst up to higher speeds if necessary?

- Yes. ExpressRoute circuits are configured to allow you to burst up to two times the bandwidth limit you procured for no additional cost. Check with your service provider to see if they support this capability. This is not for a sustained period of time and is not guaranteed.

Can I use the same private network connection with virtual network and other Azure services simultaneously?

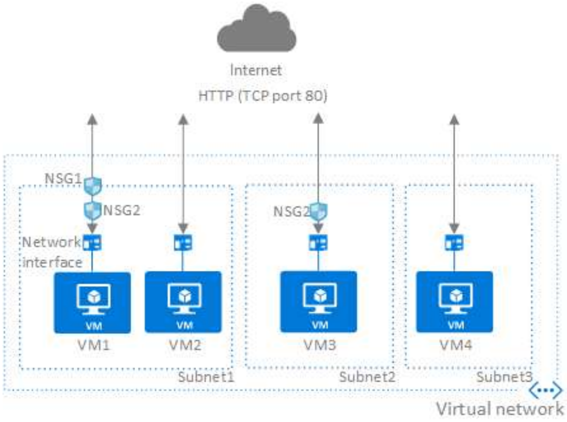
- Yes. An ExpressRoute circuit, once set up, allows you to access services within a virtual network and other Azure services simultaneously. You connect to virtual networks and to other services.

How are VNets advertised on ExpressRoute Private Peering?

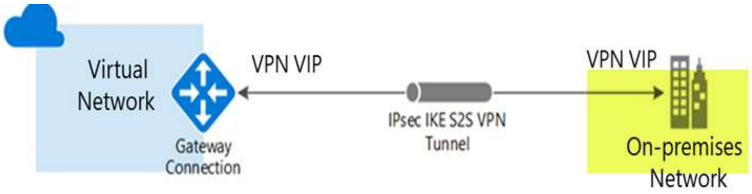
- The ExpressRoute gateway will advertise the *Address Space(s)* of the Azure VNet, you can't include/exclude at the subnet level. It is always the VNet Address Space that is advertised. Also, if VNet Peering is used and the peered VNet has "Use Remote Gateway" enabled, the Address Space of the peered VNet will also be advertised.

Filter network traffic

- **Network Security groups**: NSGs can contain multiple inbound and outbound security rules that enable you to control traffic



Configure the On-Premises VPN Device



Route network traffic

Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

- **Route tables**: You can create custom route tables with routes that control where traffic is routed to for each subnet.
- **Border gateway protocol (BGP) routes**: If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute

Choose Between Virtual Network Peering and VPN Gateways in Azure

Virtual network peering. Virtual network peering connects two Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, through private IP addresses only. No public internet is involved. You can also peer virtual networks across Azure regions (global peering).

Choose Between Virtual Network Peering and VPN Gateways in Azure

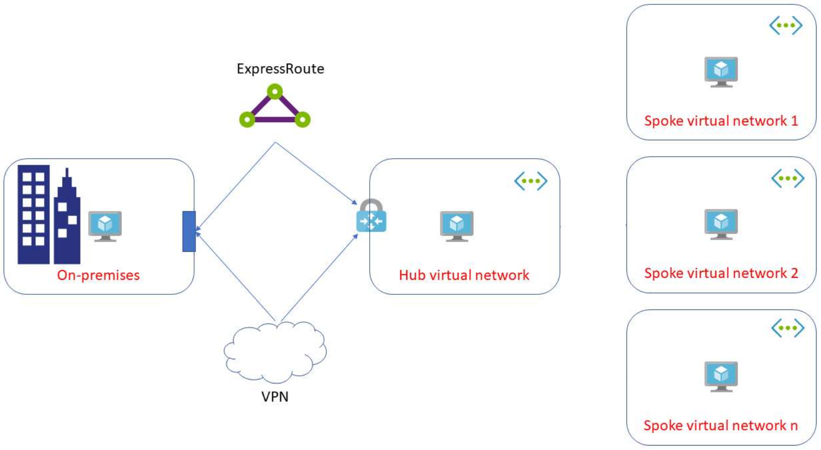
VPN gateways. A VPN gateway is a specific type of virtual network gateway that is used to send traffic between an Azure virtual network and an on-premises location over the internet. You can also use a VPN gateway to send traffic between Azure virtual networks.

Virtual network peering provides a low-latency, high-bandwidth connection. There is no gateway in the path, so there are no extra hops, ensuring low latency connections. It's useful in scenarios such as cross-region data replication and database failover. Because traffic is private and remains on the Microsoft backbone, also consider virtual network peering if you have strict data policies and want to avoid sending any traffic over the internet.

Gateway Transit

- Gateway transit enables you to use a peered virtual network's gateway for connecting to on-premises, instead of creating a new gateway for connectivity. Gateway transit allows you to share an ExpressRoute or VPN gateway with all peered virtual networks and lets you manage the connectivity in one place
- With gateway transit enabled on virtual network peering, you can create a transit virtual network that contains your VPN gateway, Network Virtual Appliance, and other shared services. As your organization grows with new applications or business units and as you spin up new virtual networks, you can connect to your transit virtual network using peering. This prevents adding complexity to your network and reduces management overhead of managing multiple gateways and other appliances.

Gateway Transit



What is the same?

Virtual network peering and VPN gateways **both** support the following connection types:

- Virtual networks in different regions.
- Virtual networks in different Azure Active Directory tenants.
- Virtual networks in different Azure subscriptions.
- Virtual networks that use a mix of Azure deployment models (Resource Manager and classic).

Item	Virtual Network Peering	VPN Gateway
Limits	Up to 500 virtual network peerings per virtual network	One VPN gateway per virtual network. The maximum number of tunnels per gateway depends on the gateway SKU
Pricing	Ingress/Egress	Hourly + Egress
Encryption	Software-level encryption is recommended.	Custom IPsec/IKE policy can be applied to new or existing connections.
Bandwidth limitations	None	Varies based on SKU
Private?	Yes. Routed through Microsoft's backbone	Public IP involved
Transitive relationship	Non-transitive	If virtual networks are connected via VPN gateways and BGP is enabled in the virtual network connections, transitivity works

Item	Virtual Network Peering	VPN Gateway
Initial setup time	Fast (1-2 minutes)	~30 minutes
Use case scenarios	Data replication, database failover, and other scenarios needing frequent backups of large data.	Encryption-specific scenarios that are not latency sensitive and do not need high throughout

Peering Types

Virtual network peering connects virtual networks in the same Azure region, such as two virtual networks in North Europe.

Global virtual network peering connects virtual networks that are in different Azure regions, such as a virtual network in North Europe and a virtual network in West Europe.

Cross-subscription virtual network peering

- You can use virtual network peering even when both virtual networks are in different subscriptions. This might be necessary for mergers and acquisitions or to connect virtual networks in subscriptions that different departments manage.

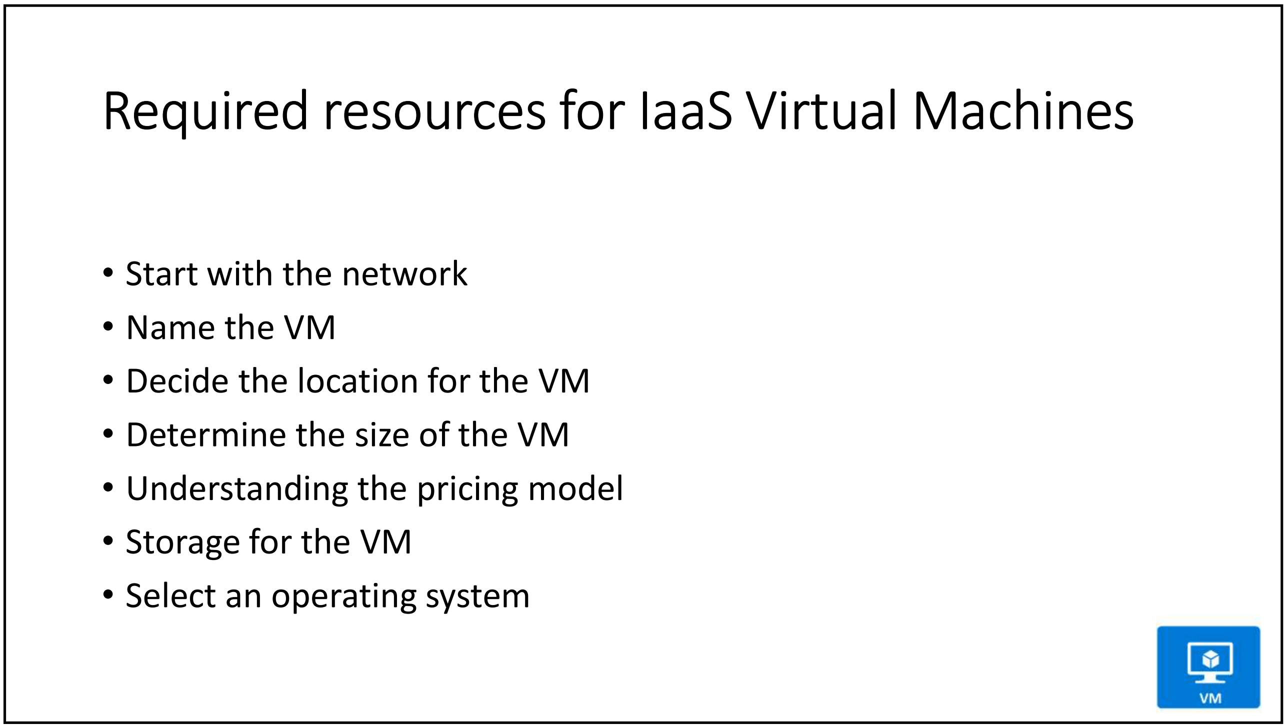
Module 3:
Planning and Implementing Virtual Machines

Topics Covered

□Planning VM deployments

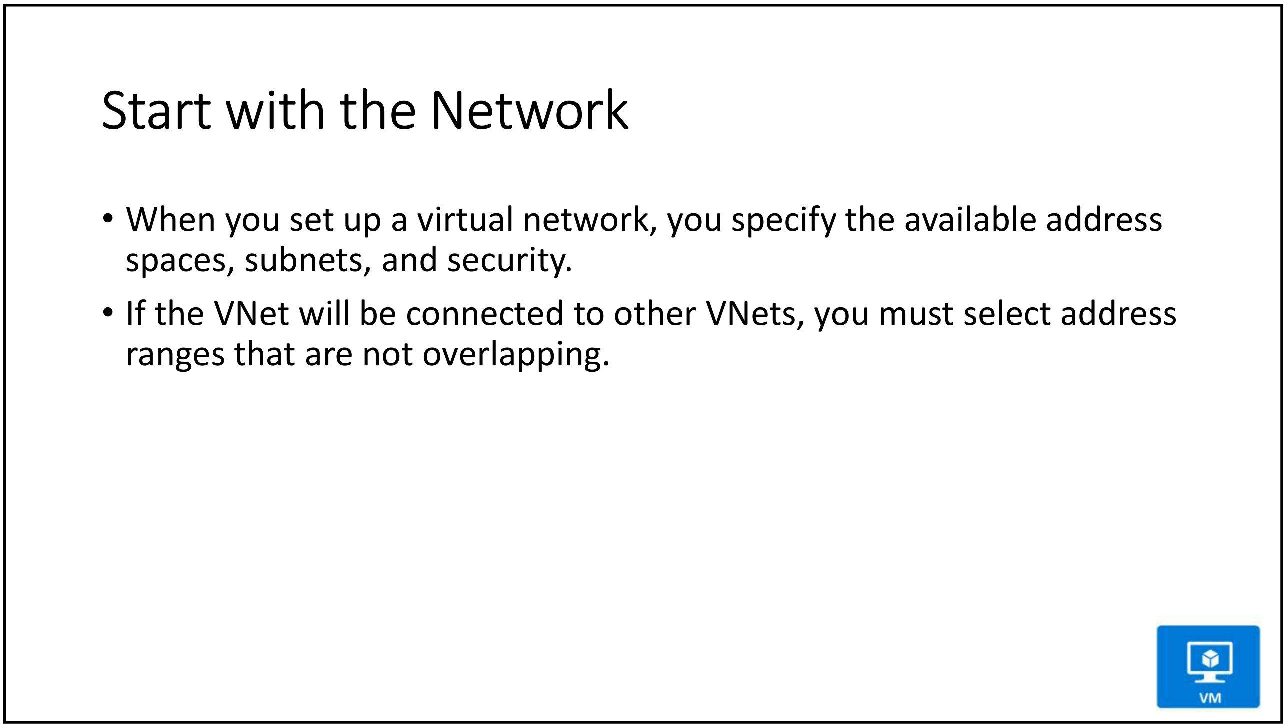
□Planning High Availability for VMs

□Planning and implementing VM Scale Sets (VMSS)



Required resources for IaaS Virtual Machines

- Start with the network
- Name the VM
- Decide the location for the VM
- Determine the size of the VM
- Understanding the pricing model
- Storage for the VM
- Select an operating system



Start with the Network

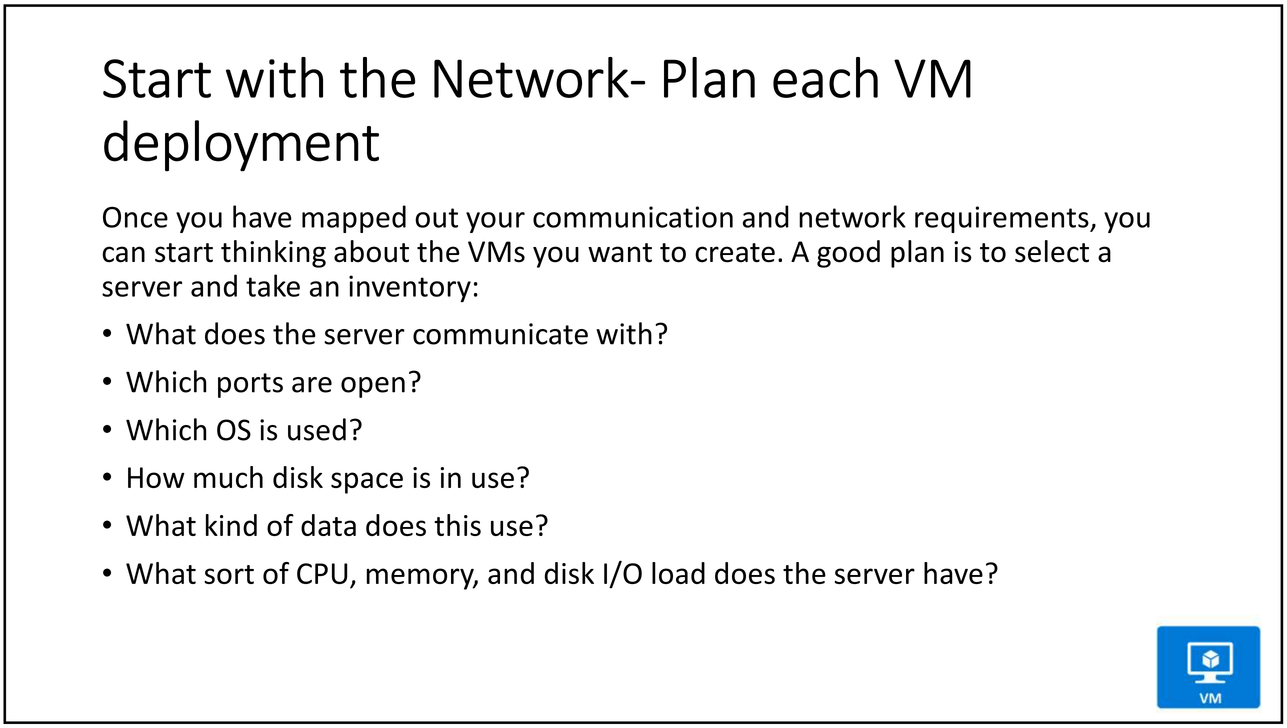
- When you set up a virtual network, you specify the available address spaces, subnets, and security.
- If the VNet will be connected to other VNets, you must select address ranges that are not overlapping.

Start with the Network- Segregate the network

After deciding the virtual network address space(s), you can create one or more subnets for your virtual network. You do this to break up your network into more manageable sections. For example, you might assign 10.1.0.0/16 to VMs, 10.2.0.0/16 to back-end services, and 10.3.0.0/16 to SQL Server VMs.

Start with the Network- Secure the network

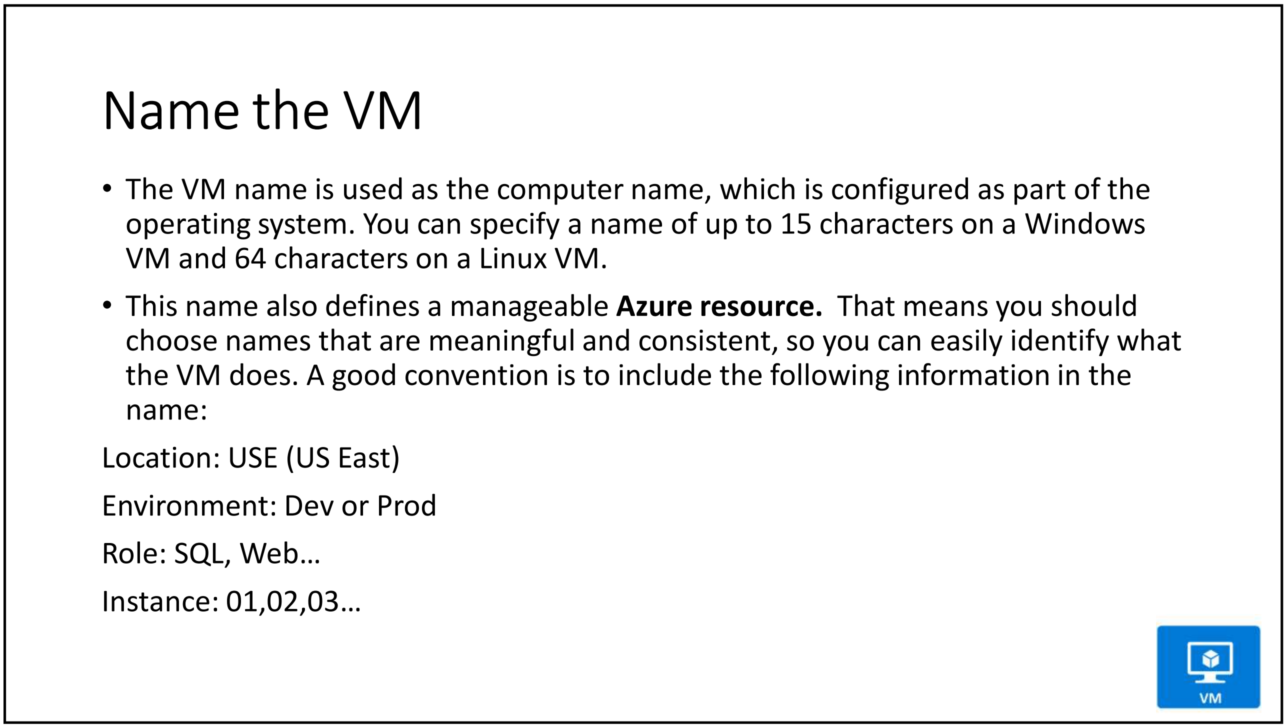
By default, there is no security boundary between subnets, so services in each of these subnets can talk to one another. However, you can set up Network Security Groups (NSGs), which allow you to control the traffic flow to and from subnets and to and from VMs. NSGs act as software firewalls, applying custom rules to each inbound or outbound request at the network interface and subnet level. This allows you to fully control every network request coming in or out of the VM.



Start with the Network- Plan each VM deployment

Once you have mapped out your communication and network requirements, you can start thinking about the VMs you want to create. A good plan is to select a server and take an inventory:

- What does the server communicate with?
- Which ports are open?
- Which OS is used?
- How much disk space is in use?
- What kind of data does this use?
- What sort of CPU, memory, and disk I/O load does the server have?



Name the VM

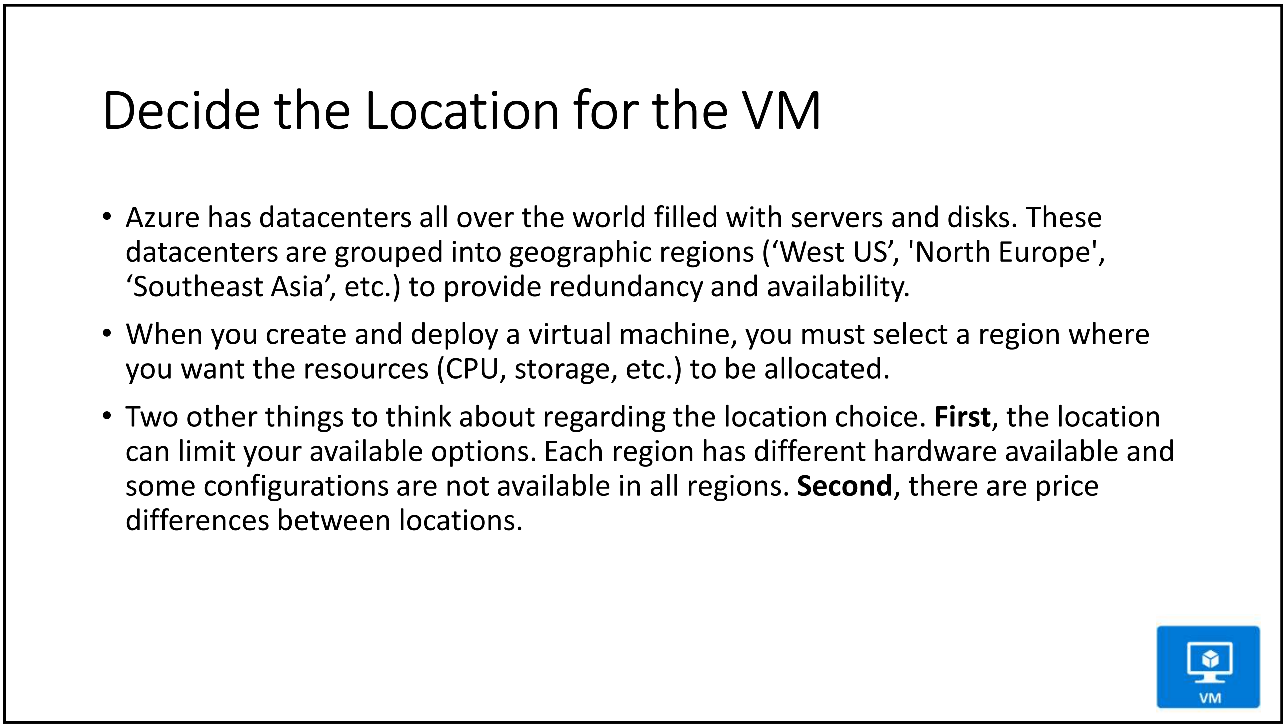
- The VM name is used as the computer name, which is configured as part of the operating system. You can specify a name of up to 15 characters on a Windows VM and 64 characters on a Linux VM.
- This name also defines a manageable **Azure resource.** That means you should choose names that are meaningful and consistent, so you can easily identify what the VM does. A good convention is to include the following information in the name:

Location: USE (US East)

Environment: Dev or Prod

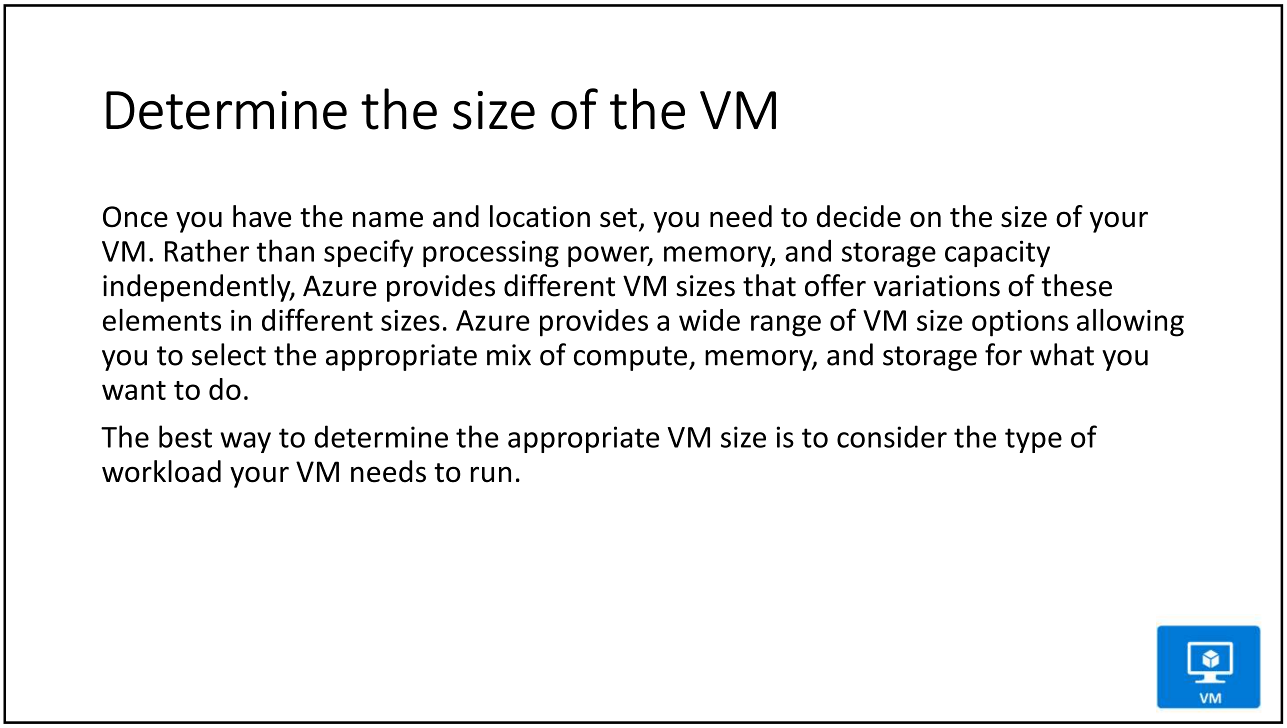
Role: SQL, Web…

Instance: 01,02,03…



Decide the Location for the VM

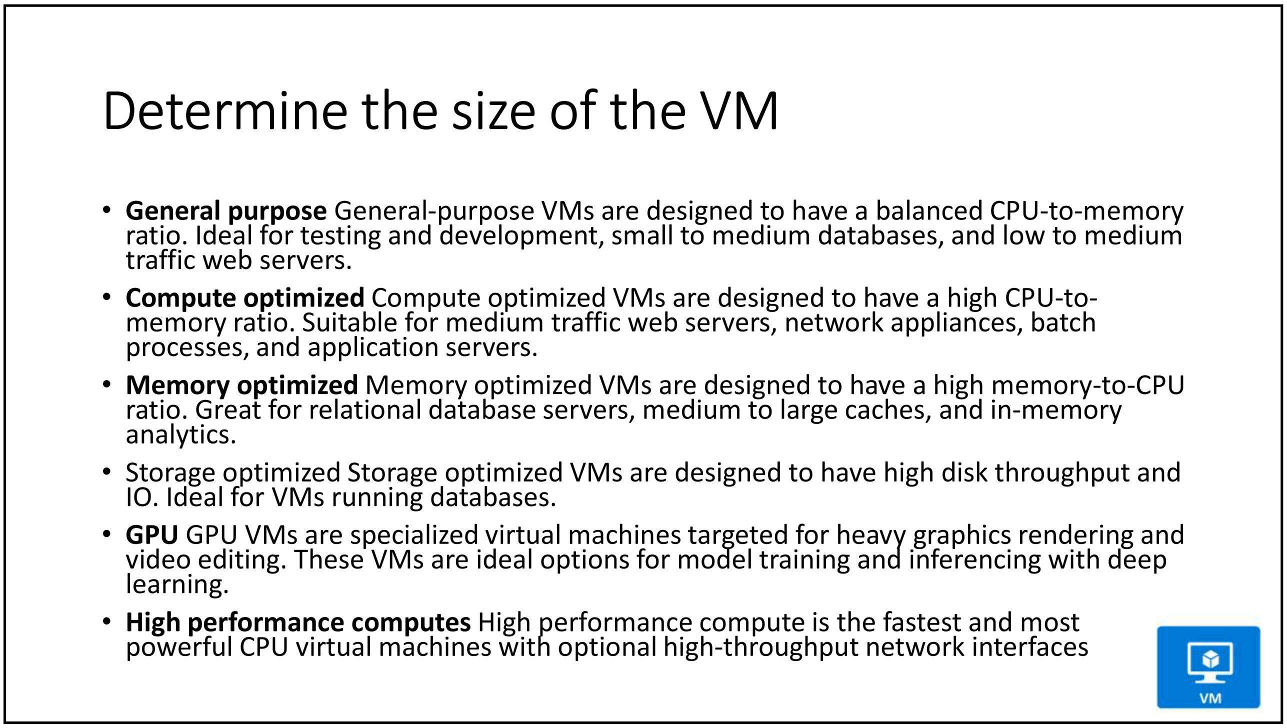
- Azure has datacenters all over the world filled with servers and disks. These datacenters are grouped into geographic regions (‘West US’, 'North Europe', ‘Southeast Asia’, etc.) to provide redundancy and availability.
- When you create and deploy a virtual machine, you must select a region where you want the resources (CPU, storage, etc.) to be allocated.
- Two other things to think about regarding the location choice. **First**, the location can limit your available options. Each region has different hardware available and some configurations are not available in all regions. **Second**, there are price differences between locations.



Determine the size of the VM

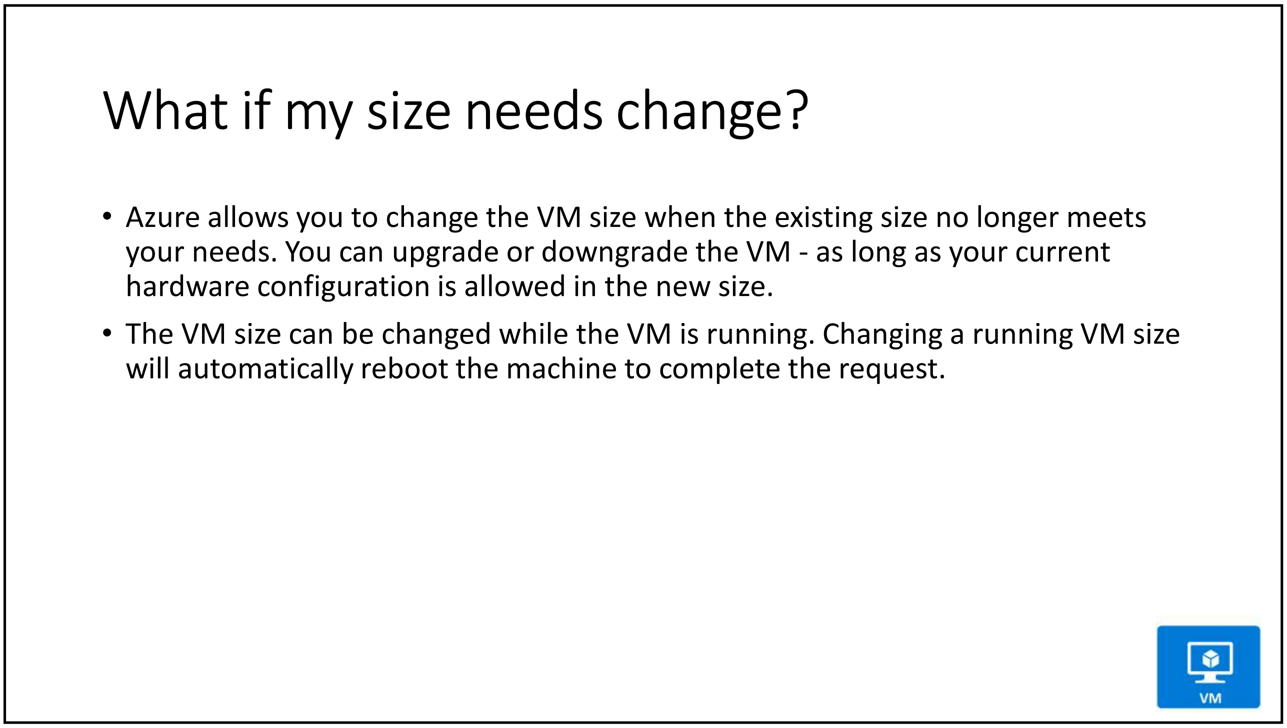
Once you have the name and location set, you need to decide on the size of your VM. Rather than specify processing power, memory, and storage capacity independently, Azure provides different VM sizes that offer variations of these elements in different sizes. Azure provides a wide range of VM size options allowing you to select the appropriate mix of compute, memory, and storage for what you want to do.

The best way to determine the appropriate VM size is to consider the type of workload your VM needs to run.



Determine the size of the VM

- **General purpose** General-purpose VMs are designed to have a balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
- **Compute optimized** Compute optimized VMs are designed to have a high CPU-to-memory ratio. Suitable for medium traffic web servers, network appliances, batch processes, and application servers.
- **Memory optimized** Memory optimized VMs are designed to have a high memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
- Storage optimized Storage optimized VMs are designed to have high disk throughput and IO. Ideal for VMs running databases.
- **GPU** GPU VMs are specialized virtual machines targeted for heavy graphics rendering and video editing. These VMs are ideal options for model training and inferencing with deep learning.
- **High performance computes** High performance compute is the fastest and most powerful CPU virtual machines with optional high-throughput network interfaces



What if my size needs change?

- Azure allows you to change the VM size when the existing size no longer meets your needs. You can upgrade or downgrade the VM - as long as your current hardware configuration is allowed in the new size.
- The VM size can be changed while the VM is running. Changing a running VM size will automatically reboot the machine to complete the request.

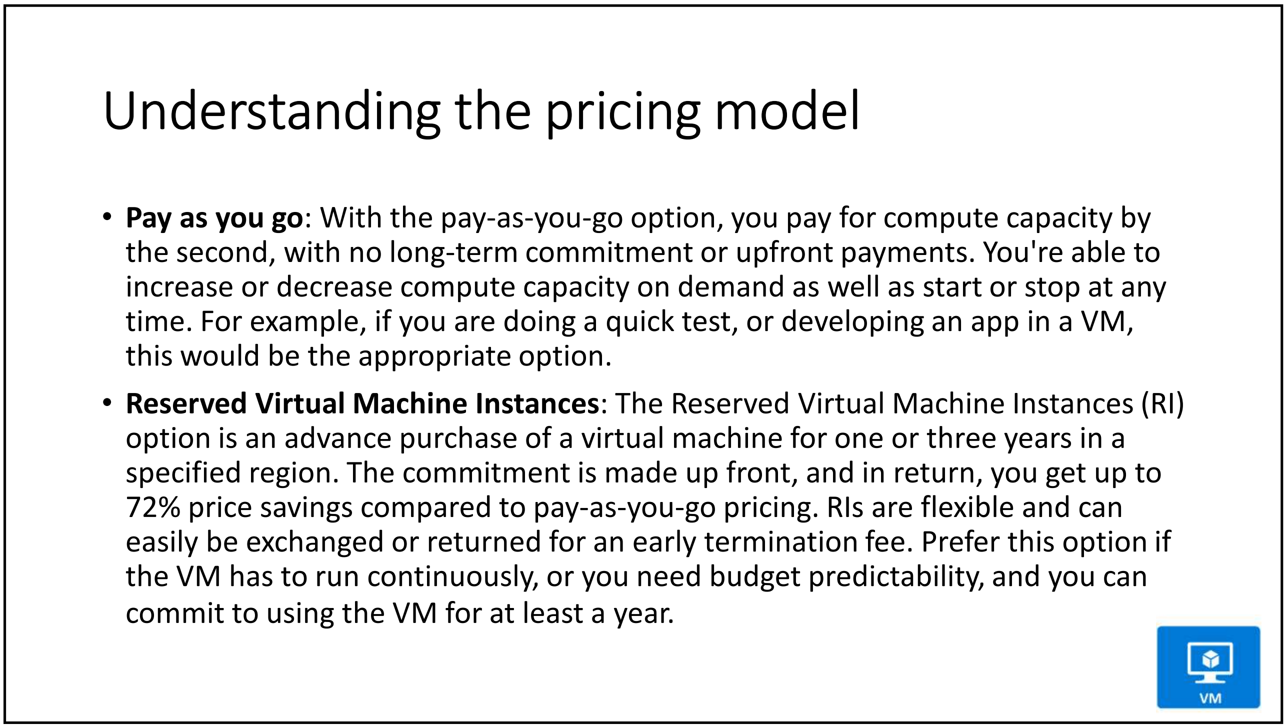
Understanding the pricing model

There are two separate costs the subscription will be charged for every VM: **compute** and **storage**. By separating these costs, you scale them independently and only pay for what you need.

- **Compute costs** - Compute expenses are priced on a per-hour basis but billed on a per-minute basis. For example, you are only charged for 55 minutes of usage if the VM is deployed for 55 minutes. You are not charged for compute capacity if you stop and deallocate the VM. The hourly price varies based on the VM size and OS you select. The cost for a VM includes the charge for the Windows operating system. Linux-based instances are cheaper because there is no operating system license charge.

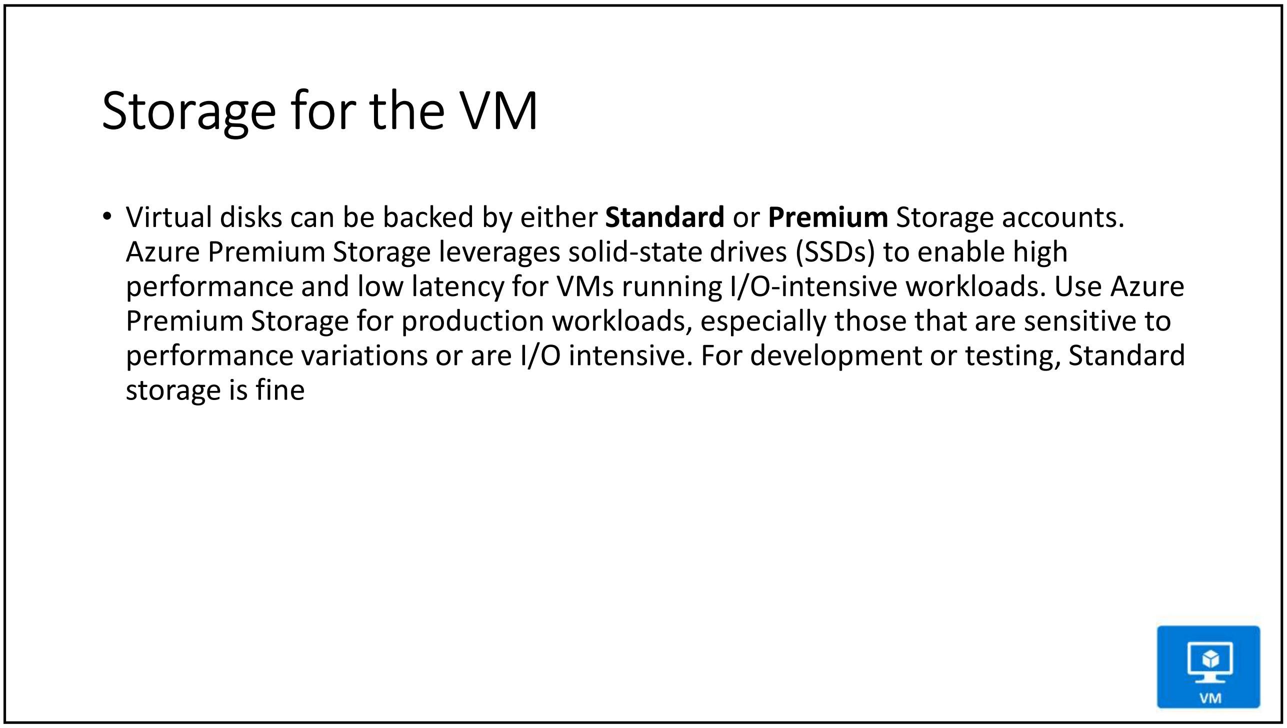
Understanding the pricing model

- **Storage costs** - You are charged separately for the storage the VM uses. The status of the VM has no relation to the storage charges that will be incurred; even if the VM is stopped/deallocated and you aren't billed for the running VM, you will be charged for the storage used by the disks.



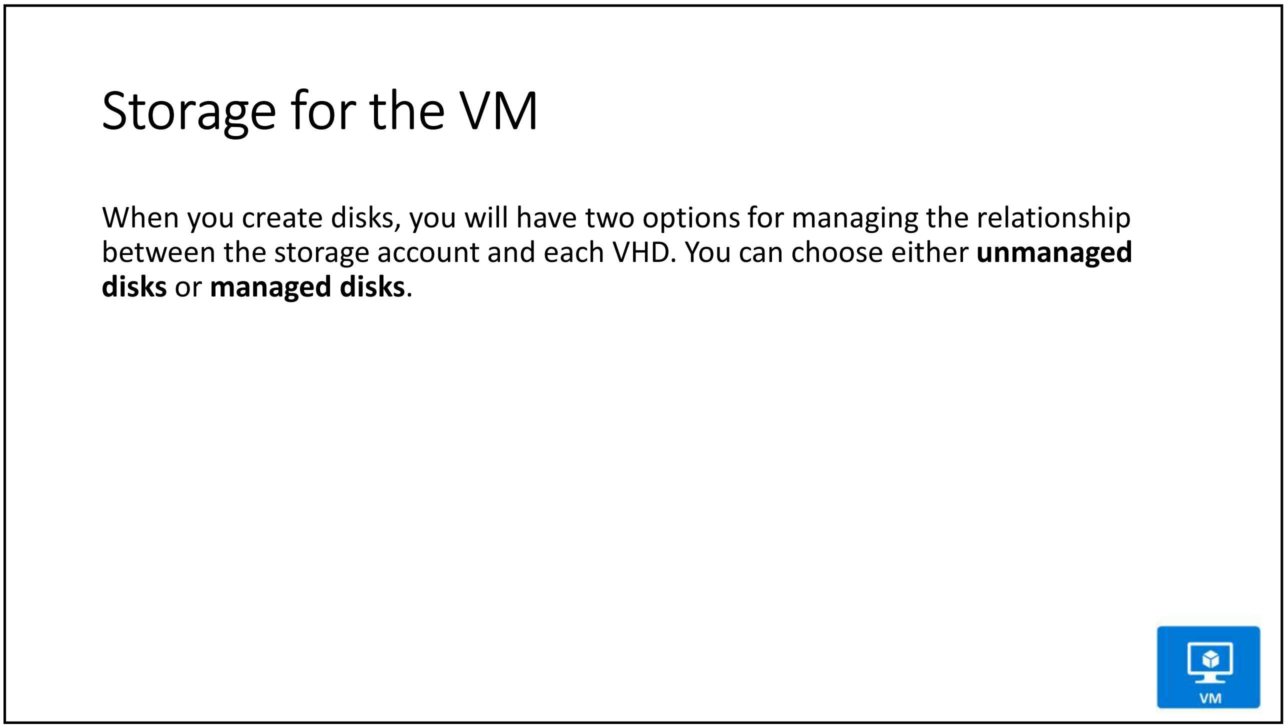
Understanding the pricing model

- **Pay as you go**: With the pay-as-you-go option, you pay for compute capacity by the second, with no long-term commitment or upfront payments. You're able to increase or decrease compute capacity on demand as well as start or stop at any time. For example, if you are doing a quick test, or developing an app in a VM, this would be the appropriate option.
- **Reserved Virtual Machine Instances**: The Reserved Virtual Machine Instances (RI) option is an advance purchase of a virtual machine for one or three years in a specified region. The commitment is made up front, and in return, you get up to 72% price savings compared to pay-as-you-go pricing. RIs are flexible and can easily be exchanged or returned for an early termination fee. Prefer this option if the VM has to run continuously, or you need budget predictability, and you can commit to using the VM for at least a year.



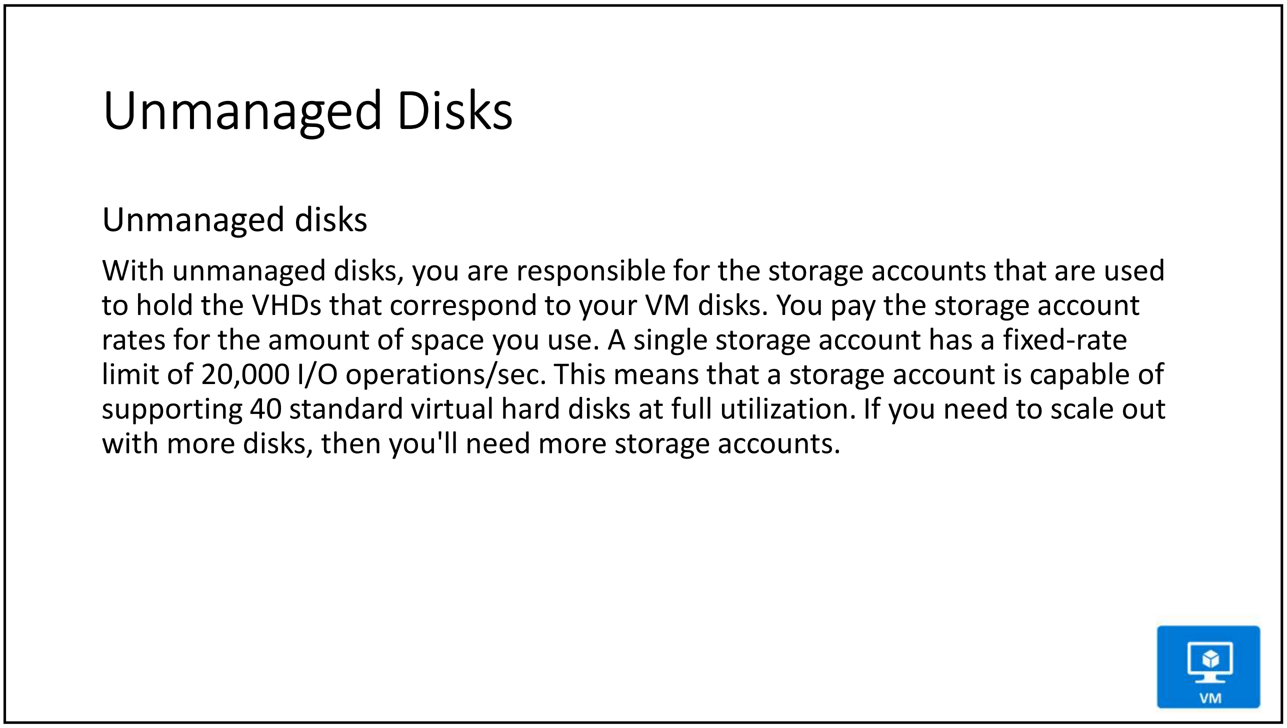
Storage for the VM

- Virtual disks can be backed by either **Standard** or **Premium** Storage accounts. Azure Premium Storage leverages solid-state drives (SSDs) to enable high performance and low latency for VMs running I/O-intensive workloads. Use Azure Premium Storage for production workloads, especially those that are sensitive to performance variations or are I/O intensive. For development or testing, Standard storage is fine



Storage for the VM

When you create disks, you will have two options for managing the relationship between the storage account and each VHD. You can choose either **unmanaged disks** or **managed disks**.



Unmanaged Disks

Unmanaged disks

With unmanaged disks, you are responsible for the storage accounts that are used to hold the VHDs that correspond to your VM disks. You pay the storage account rates for the amount of space you use. A single storage account has a fixed-rate limit of 20,000 I/O operations/sec. This means that a storage account is capable of supporting 40 standard virtual hard disks at full utilization. If you need to scale out with more disks, then you'll need more storage accounts.

Managed Disks

Managed disks

Managed disks are the newer and recommended disk storage model. They solve this complexity by putting the burden of managing the storage accounts onto Azure. You specify the size of the disk, up to 4 TB, and Azure creates and manages both the disk and the storage.

Disk Types

Standard HDD Managed Disks

- Standard HDD Managed Disks use Hard Disk Drive (HDD) based Storage media. They are best suited for dev/test and other infrequent access workloads that are less sensitive to performance variability.

Standard SSD Managed Disks

- Standard SSD Managed Disks, a low-cost SSD offering, are optimized for test and entry-level production workloads requiring consistent latency. Standard SSD Managed Disks deliver lower latency compared to Standard HDDs, while improving reliability and scalability for your applications, and are available with all Azure VM sizes. Standard SSD Managed Disks can be easily upgraded to Premium SSD Managed Disks for more demanding and latency-sensitive enterprise workloads.

Disk Types

Premium SSD Managed Disks

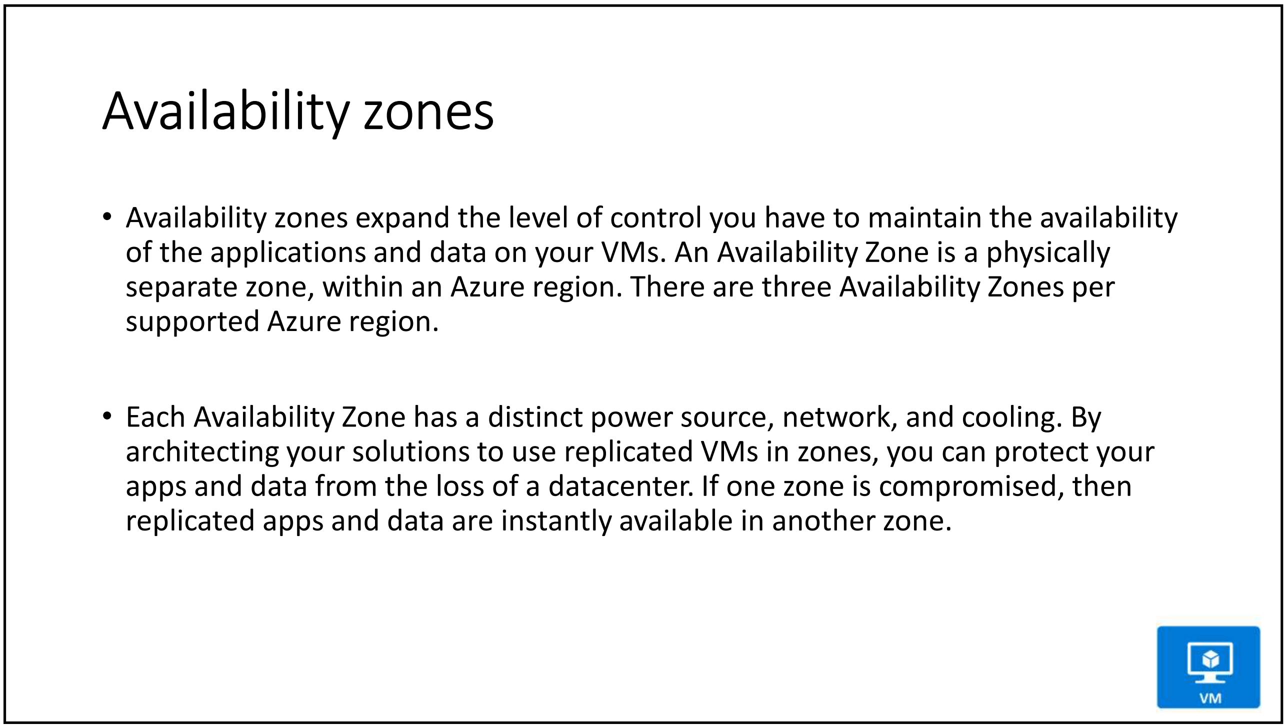
- Premium SSD Managed Disks are high performance Solid State Drive (SSD) based Storage designed to support I/O intensive workloads with significantly high throughput and low latency.

Ultra Disk

- Ultra Disk is our next generation high performance Solid State Drive (SSD) with configurable performance attributes that provides the lowest latency and consistent high IOPS/throughput. Ultra Disk offers unprecedented and extremely scalable performance with sub-millisecond latency. As a customer you can start small on IOPS and throughput and adjust your performance as your workload becomes more IO intensive.

Select an operating system

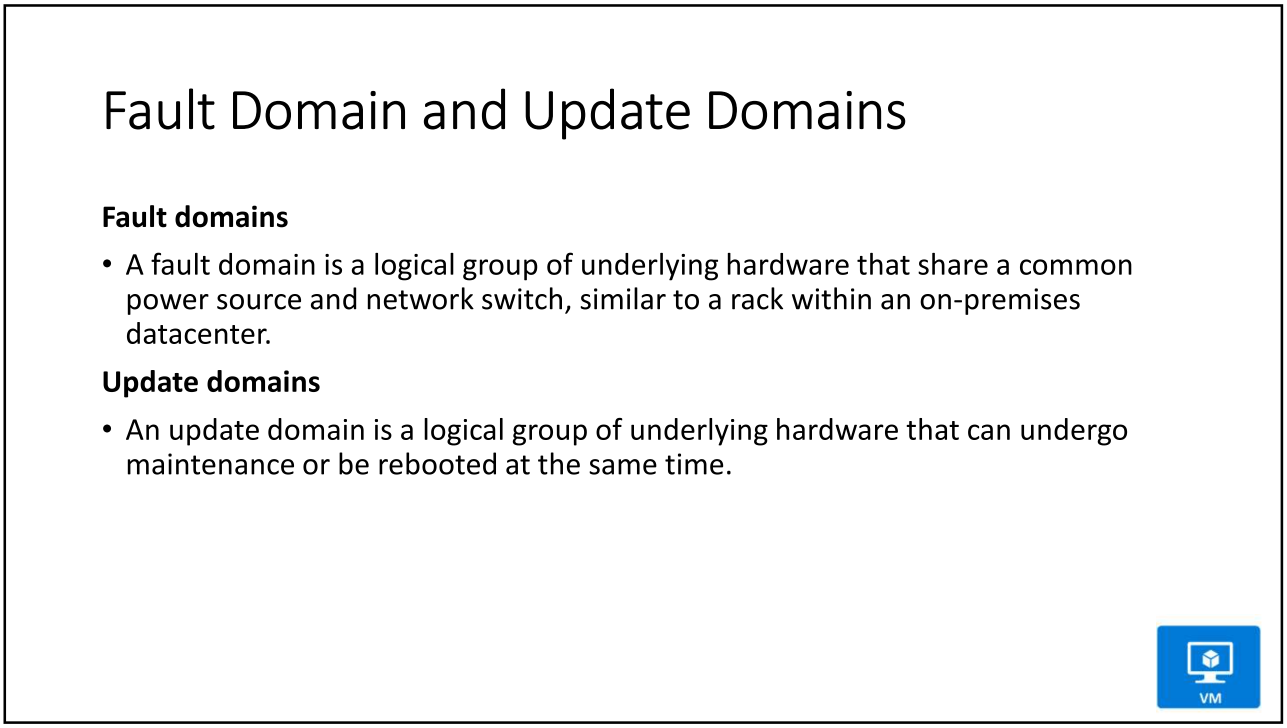
- Azure provides a variety of OS images that you can install into the VM, including several versions of Windows and flavors of Linux.
- You can search the Azure Marketplace for more sophisticated install images that include the OS and popular software tools installed for specific scenarios. For example, if you needed a new WordPress site, the standard technology stack would consist of a Linux server, Apache web server, a MySQL database, and PHP. Instead of setting up and configuring each component, you can leverage a Marketplace image and install the entire stack all at once.
- If you can't find a suitable OS image, you can create your disk image with what you need, upload it to Azure storage, and use it to create an Azure VM. Keep in mind that Azure only supports 64-bit operating systems.



Availability zones

- Availability zones expand the level of control you have to maintain the availability of the applications and data on your VMs. An Availability Zone is a physically separate zone, within an Azure region. There are three Availability Zones per supported Azure region.

- Each Availability Zone has a distinct power source, network, and cooling. By architecting your solutions to use replicated VMs in zones, you can protect your apps and data from the loss of a datacenter. If one zone is compromised, then replicated apps and data are instantly available in another zone.



Fault Domain and Update Domains

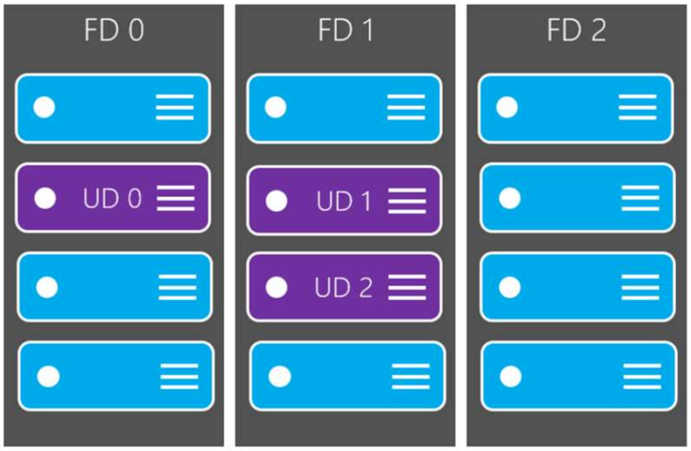
Fault domains

- A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premises datacenter.

Update domains

- An update domain is a logical group of underlying hardware that can undergo maintenance or be rebooted at the same time.

Fault Domain and Update Domains



Virtual Machines Scale Sets

- Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule.
- There is no cost for the scale set itself, you only pay for each VM instance that you create. Virtual machines in a scale set can be deployed across multiple update domains and fault domains to maximize availability and resilience to outages due to data center outages, and planned or unplanned maintenance events.

Availability Sets

- An availability set is a logical grouping of VMs within a datacenter that allows Azure to understand how your application is built to provide for redundancy and availability.
- It is recommended that two or more VMs are created within an availability set to provide for a highly available application and to meet the 99.95% Azure SLA. There is no cost for the Availability Set itself, you only pay for each VM instance that you create.
- In an availability set, VMs are automatically distributed across these fault domains. This approach limits the impact of potential physical hardware failures, network outages, or power interruptions.

Azure Dedicated Hosts

Azure Dedicated Host is a service that provides physical servers - able to host one or more virtual machines - dedicated to one Azure subscription. Dedicated hosts are the same physical servers used in our data centers, provided as a resource. You can provision dedicated hosts within a region, availability zone, and fault domain. Then, you can place VMs directly into your provisioned hosts, in whatever configuration best meets your needs.

Benefits

- Hardware isolation at the physical server level
- Control over maintenance events initiated by the Azure platform

Azure Disk Encryption

The primary encryption-based disk protection technologies for Azure VMs are:

- Storage Service Encryption (SSE)
- Azure Disk Encryption (ADE)

Storage Service Encryption is performed on the physical disks in the data center. If someone were to directly access the physical disk the data would be encrypted. When the data is accessed from the disk, it is decrypted and loaded into memory.

Azure Disk Encryption encrypts the virtual machine's virtual hard disks (VHDs). If VHD is protected with ADE, the disk image will only be accessible by the virtual machine that owns the disk.

Storage Service Encryption

- Azure Storage Service Encryption (SSE) is an encryption service built into Azure used to protect data at rest. The Azure storage platform automatically encrypts data before it's stored to several storage services, including Azure Managed Disks. Encryption is enabled by default using 256-bit AES encryption.
- Storage Service Encryption is enabled for all new and existing storage accounts and cannot be disabled. Your data is secured by default; you don't need to modify your code or applications to take advantage of Storage Service Encryption.
- Storage Service Encryption does not affect the performance of Azure storage services.

Azure Disk Encryption

- Azure Disk Encryption (ADE) is managed by the VM owner. It controls the encryption of Windows and Linux VM-controlled disks, using **BitLocker** on Windows VMs and **DM-Crypt** on Linux VMs. BitLocker Drive Encryption is a data protection feature that integrates with the operating system, and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Similarly, DM-Crypt encrypts data at rest for Linux before writing to storage.
- ADE ensures that all data on VM disks are encrypted at rest in Azure storage, and ADE is required for VMs backed up to the Recovery Vault.
- ADE is integrated with Azure Key Vault for the management of these disk-encryption keys and secrets.

VM

Module 4:
Azure Automation

Topics Covered

□Azure Resource Manager Templates

□QuickStart Templates

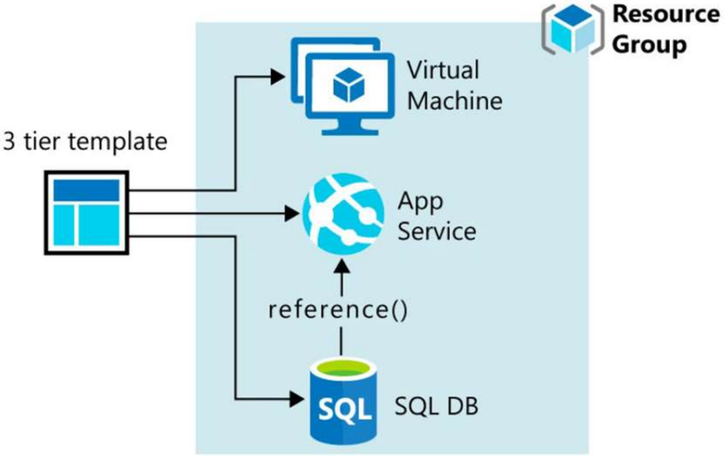
□VM Templates

□Azure Runbooks

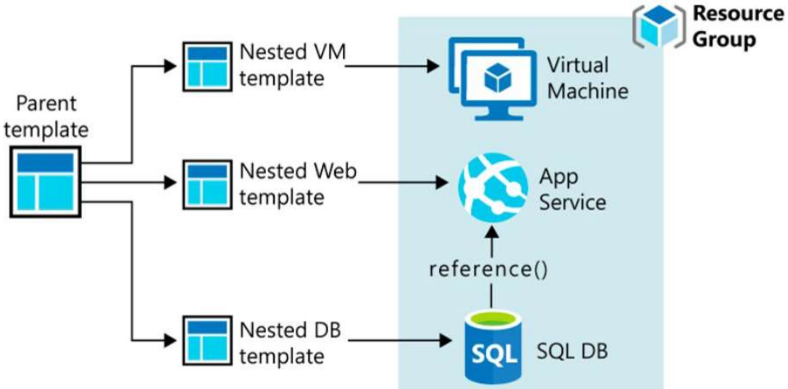
Azure Resource Manager Templates

- Azure Resource Manager is the interface for managing and organizing cloud resources. Think of Resource Manager as a way to deploy cloud resources.
- If you're familiar with Azure resource groups, you know that they enable you to treat sets of related resources as a single unit. Resource Manager is what organizes the resource groups that let you deploy, manage, and delete all of the resources together in a single action.

Azure Resource Manager Templates



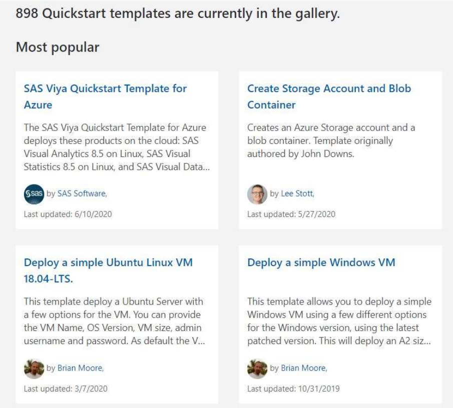
Azure Resource Manager Templates



Azure Quickstart Templates

Azure Quickstart templates are Resource Manager templates that are provided by the Azure community. Quickstart templates are available on GitHub.

https://azure.microsoft.com/resources/templates/



898 Quickstart templates are currently in the gallery.

Most popular

SAS Viya Quickstart Template for Azure

The SAS Viya Quickstart Template for Azure deploys these products on the cloud: SAS Visual Analytics 8.5 on Linux, SAS Visual Statistics 8.5 on Linux, and SAS Visual Data...

by SAS Software,

Last updated: 6/10/2020

Create Storage Account and Blob Container

Creates an Azure Storage account and a blob container. Template originally authored by John Downs.

by Lee Stott,

Last updated: 5/27/2020

Deploy a simple Ubuntu Linux VM 18.04-LTS.

This template deploy a Ubuntu Server with a few options for the VM. You can provide the VM Name, OS Version, VM size, admin username and password. As default the V...

by Brian Moore,

Last updated: 3/7/2020

Deploy a simple Windows VM

This template allows you to deploy a simple Windows VM using a few different options for the Windows version, using the latest patched version. This will deploy an A2 siz...

by Brian Moore,

Last updated: 10/31/2019

Runbooks in Azure Automation

- A **runbook** is a compilation of routine procedures and operations that an administrator wants to automate.
- Automation executes your runbooks based on the logic defined inside them.
- Starting a runbook in Azure Automation creates a job, which is a single execution instance of the runbook. Each job accesses Azure resources by making a connection to your Azure subscription. The job can only access resources in your data center if those resources are accessible from the public cloud.

Module 5:

High Availability, Traffic Management and Firewall Security

VM

Topics Covered

❑Azure Load Balancer
❑Application Gateway
❑Azure Firewall
❑Traffic Manager
❑Network Security Groups
❑Application Security Groups
❑Azure Bastion

Implement Azure Load Balancer

- With Azure Load Balancer, you can spread user requests across multiple virtual machines or other services. That way, you can scale the app to larger sizes than a single virtual machine can support, and you ensure that users get service, even when a virtual machine fails.

Implement Azure Load Balancer

Load balancers use a hash-based distribution algorithm. By default, a five-tuple hash is used to map traffic to available servers. The hash is made from the following elements:

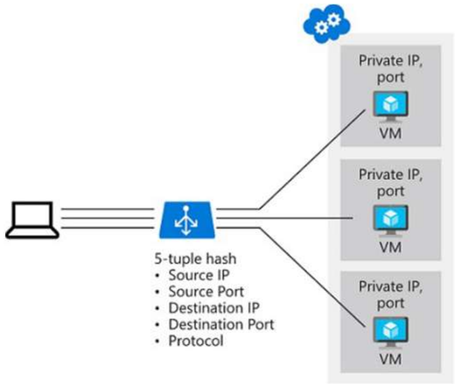
- **Source IP**: The IP address of the requesting client.
- **Source port**: The port of the requesting client.
- **Destination IP**: The destination IP of the request.
- **Destination port**: The destination port of the request.
- **Protocol type**: The specified protocol type, TCP or UDP.

Implement Azure Load Balancer

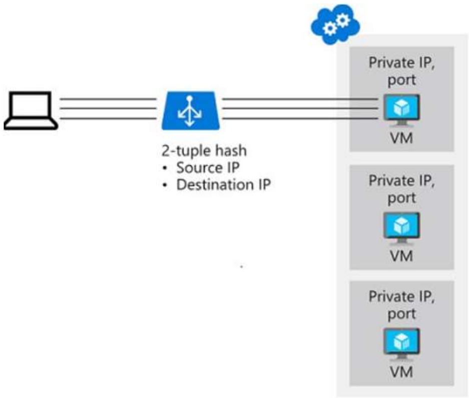
- **Source IP affinity**. This distribution mode is also known as session affinity or client IP affinity. To map traffic to the available servers, the mode uses a two-tuple hash (from the source IP address and destination IP address) or three-tuple hash (from the source IP address, destination IP address, and protocol type). The hash ensures that requests from a specific client are always sent to the same virtual machine behind the load balancer.

Traffic Distribution

5-Tuple



Source IP affinity

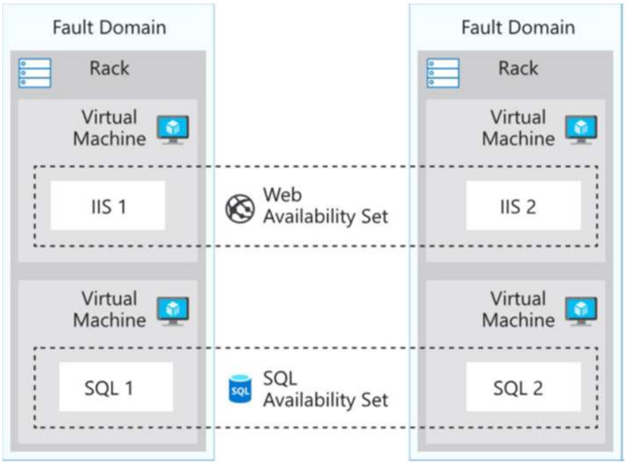


Implement Azure Load Balancer

Availability sets

- An availability set is a logical grouping that you use to isolate virtual machine resources from each other when they're deployed. Azure ensures that the virtual machines you put in an availability set run across multiple physical servers, compute racks, storage units, and network switches. If there's a hardware or software failure, only a subset of your virtual machines is affected.

Implement Azure Load Balancer

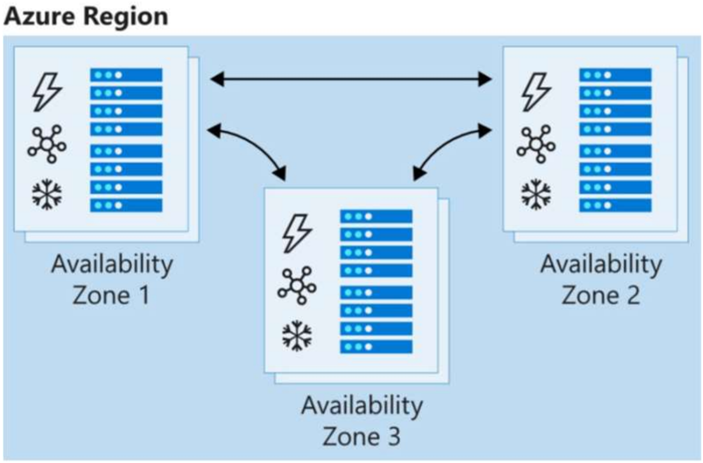


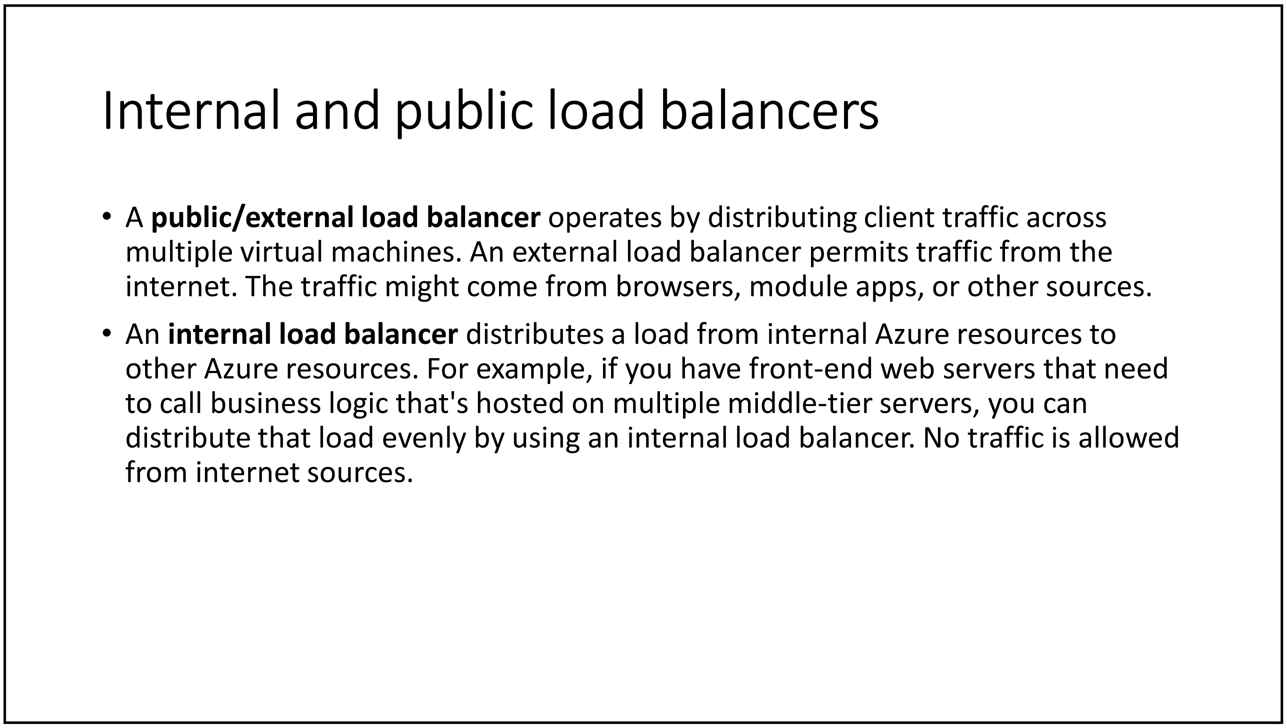
Implement Azure Load Balancer

Availability zones

- An availability zone offers groups of one or more datacenters that have independent power, cooling, and networking. The virtual machines in an availability zone are placed in different physical locations within the same region. Use this architecture when you want to ensure that, when an entire datacenter fails, you can continue to serve users.
- Availability zones don't support all virtual machine sizes and aren't available in all Azure regions. Check that they are supported in your region before you use them in your architecture.

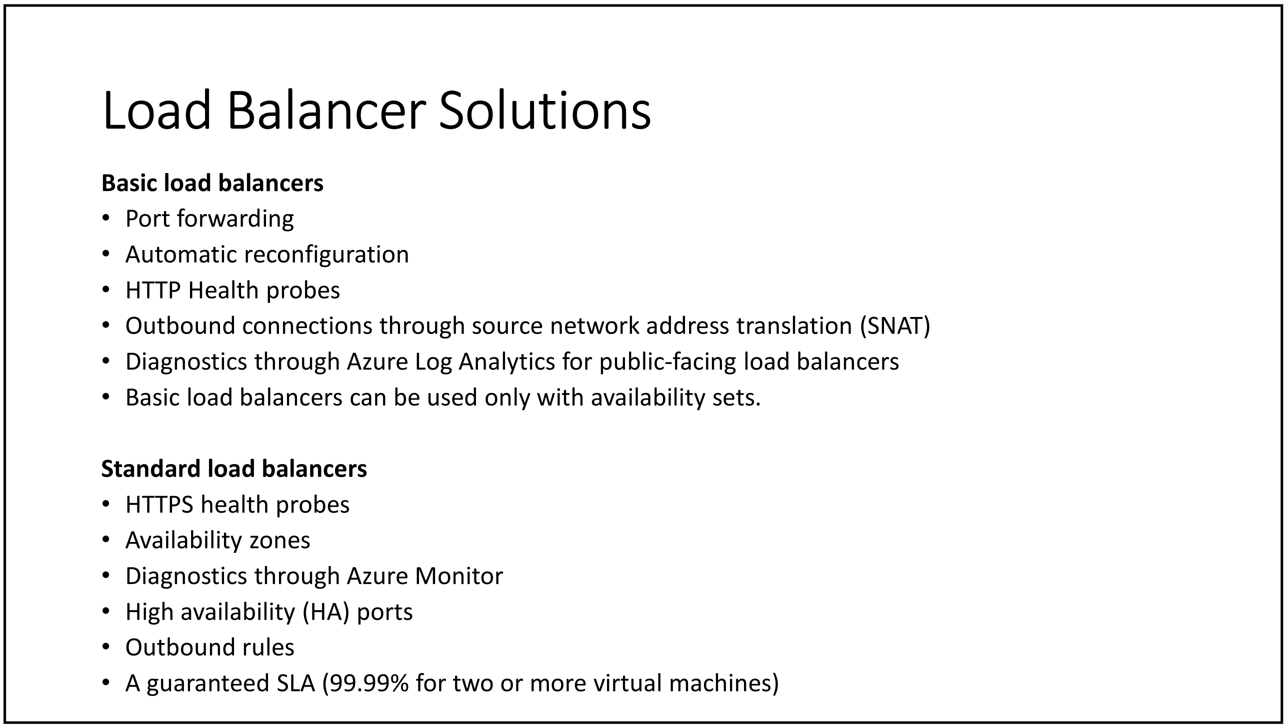
Implement Azure Load Balancer





Internal and public load balancers

- A **public/external load balancer** operates by distributing client traffic across multiple virtual machines. An external load balancer permits traffic from the internet. The traffic might come from browsers, module apps, or other sources.
- An **internal load balancer** distributes a load from internal Azure resources to other Azure resources. For example, if you have front-end web servers that need to call business logic that's hosted on multiple middle-tier servers, you can distribute that load evenly by using an internal load balancer. No traffic is allowed from internet sources.



Load Balancer Solutions

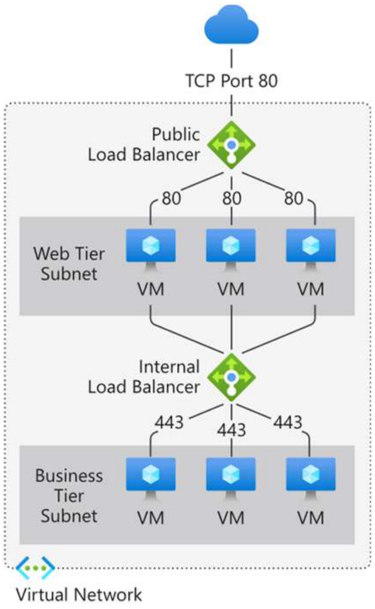
Basic load balancers

- Port forwarding
- Automatic reconfiguration
- HTTP Health probes
- Outbound connections through source network address translation (SNAT)
- Diagnostics through Azure Log Analytics for public-facing load balancers
- Basic load balancers can be used only with availability sets.

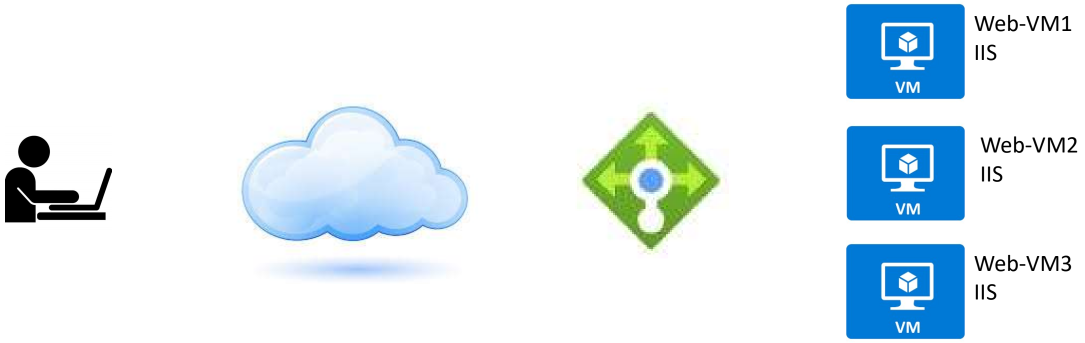
Standard load balancers

- HTTPS health probes
- Availability zones
- Diagnostics through Azure Monitor
- High availability (HA) ports
- Outbound rules
- A guaranteed SLA (99.99% for two or more virtual machines)

Traffic Distribution



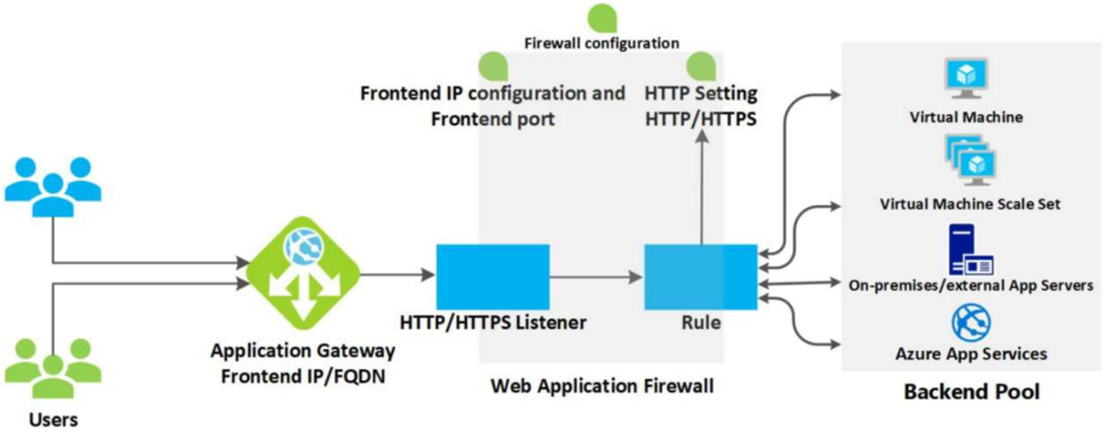
Load Balancing Demonstration



Application Gateway

- Application Gateway manages the requests from clients to a web app. Application Gateway routes traffic to a pool of web servers based on the URL of a request. This is known as application layer routing. The pool of web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers.

Application Gateway

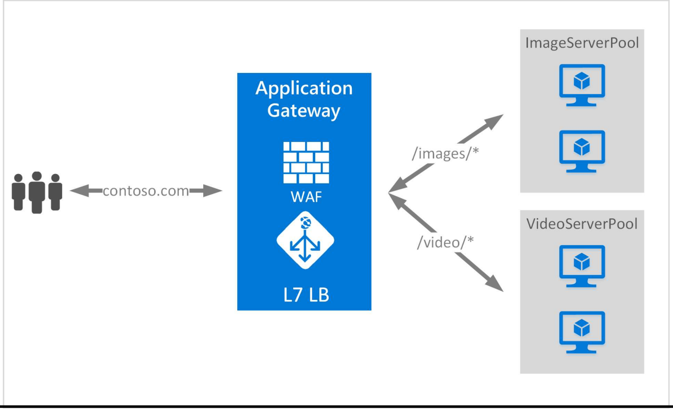


Azure Load Balancer vs Application Gateway

- The first real difference between the Azure Load Balancer and Application Gateway is that an ALB works with traffic at Layer 4, while Application Gateway handles just Layer 7 traffic, and specifically, within that, HTTP (including HTTPS and WebSockets).
- Load Balancer is free
- Application Gateway is billed per-hour, and has two tiers
- Application Gateway supports SSL termination, URL-based routing, multi-site routing, Cookie-based session affinity and Web Application Firewall (WAF) features.
- Azure Load Balancer provides basic load balancing based on 5 tuple matches.
- Load Balancer only supports endpoints hosted in Azure. Application Gateway can support any routable IP address, including on-premise resources.

Path Based Routing

Requests for http://contoso.com/video/* are routed to VideoServerPool, and http://contoso.com/images/* are routed to ImageServerPool. DefaultServerPool is selected if none of the path patterns match.

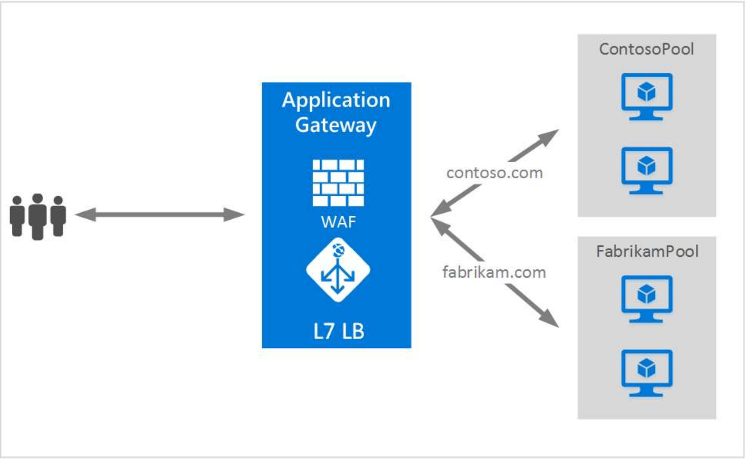


Application Gateway multiple site hosting

Multiple site hosting enables you to configure more than one web application on the same port of an application gateway. This feature allows you to configure a more efficient topology for your deployments by adding up to 100 websites to one application gateway.

Each website can be directed to its own backend pool. In the following example, application gateway serves traffic for contoso.com and fabrikam.com from two back-end server pools called ContosoServerPool and FabrikamServerPool.

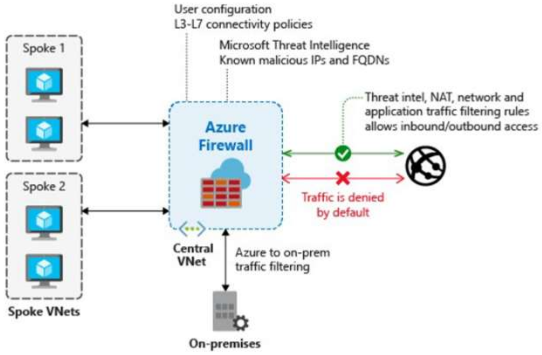
Application Gateway multiple site hosting



Azure Firewall

- Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.
- Azure Firewall has built-in high availability and unrestricted cloud scalability.
- You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network.
- The service is fully integrated with Azure Monitor for logging and analytics.

Azure Firewall

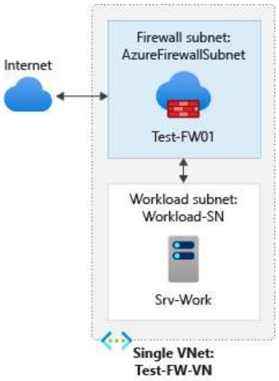

User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Spoke 1
Spoke 2
Spoke VNets
Azure Firewall
Threat intel, NAT, network and application traffic filtering rules allows inbound/outbound access
Traffic is denied by default
Central VNet
Azure to on-prem traffic filtering
On-premises

Azure Firewall features

- **Built-in high availability**. High availability is built in, so no additional load balancers are required and there's nothing you need to configure.
- **Availability Zones**. Azure Firewall can be configured during deployment to span multiple Availability Zones for increased availability.
- **Unrestricted cloud scalability**. Azure Firewall can scale up as much as you need to accommodate changing network traffic flows, so you don't need to budget for your peak traffic.
- **Application FQDN filtering rules**. You can limit outbound HTTP/S traffic or Azure SQL traffic to a specified list of fully qualified domain names (FQDN) including wild cards.
- **Network traffic filtering rules**. You can centrally create allow or deny network filtering rules by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections. Rules are enforced and logged across multiple subscriptions and virtual networks.
- **Threat intelligence**. Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed.
- **Multiple public IP addresses**. You can associate multiple public IP addresses (up to 100) with your firewall.

Azure Firewall

For production deployments, a hub and spoke model is recommended, where the firewall is in its own VNet. The workload servers are in peered VNets in the same region with one or more subnets.

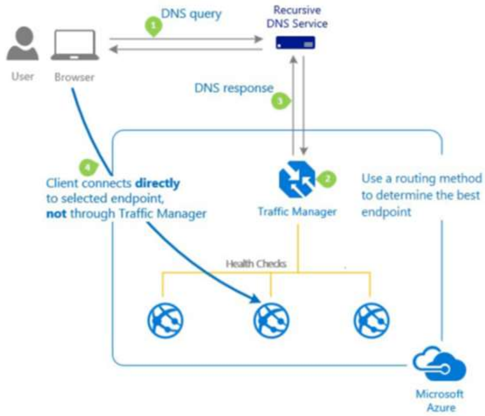


In this tutorial, you learn how to:

❑ Set up a test network environment
❑ Deploy a firewall
❑ Create a default route
❑ Configure an application rule to allow access to www.google.com
❑ Configure a network rule to allow access to external DNS servers
❑ Configure a NAT rule to allow a remote desktop to the test server
❑ Test the firewall

Azure Traffic Manager

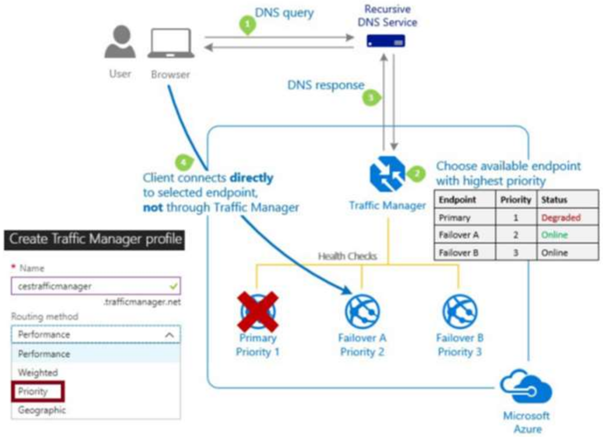
- Microsoft Azure Traffic Manager allows you to control the distribution of user traffic to your service endpoints running in different datacenters around the world.


DNS query
1
Recursive DNS Service
User
Browser
DNS response
3
4
Client connects **directly** to selected endpoint, **not** through Traffic Manager
2
Traffic Manager
Use a routing method to determine the best endpoint
Health Checks
Microsoft Azure

Priority routing

- When a Traffic Manager profile is configured for priority routing it contains a prioritized list of service endpoints. Traffic Manager sends all traffic to the primary (highest-priority) endpoint first. If the primary endpoint is not available, Traffic Manager routes the traffic to the second endpoint, and so on.

Priority routing



4 Client connects **directly** to selected endpoint, **not** through Traffic Manager

Choose available endpoint with highest priority

Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

Create Traffic Manager profile

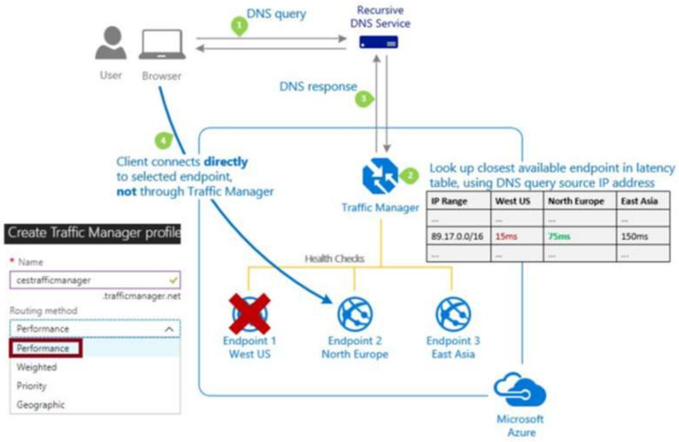
* Name: cestrafficmanager ✓ .trafficmanager.net

Routing method: Performance

Performance routing

- The Performance routing method is designed to improve the responsiveness by routing traffic to the location that is closest to the user. The closest endpoint is not necessarily measured by geographic distance. Instead Traffic Manager determines closeness by measuring network latency.
- Traffic Manager maintains an Internet Latency Table to track the round-trip time between IP address ranges and each Azure datacenter. With this method Traffic Manager looks up the source IP address of the incoming DNS request in the Internet Latency Table. Traffic Manager chooses an available endpoint in the Azure datacenter that has the lowest latency for that IP address range, then returns that endpoint in the DNS response.

Performance routing



Client connects **directly** to selected endpoint, **not** through Traffic Manager

Look up closest available endpoint in latency table, using DNS query source IP address

IP Range	West US	North Europe	East Asia
—	—	—	—
89.17.0.0/16	15ms	75ms	150ms
—	—	—	—

Create Traffic Manager profile

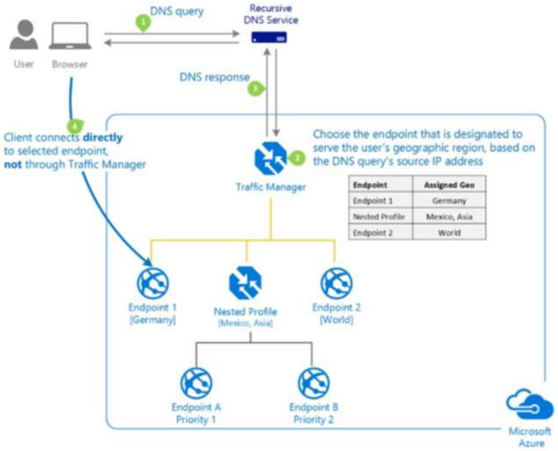
* Name: cestrafficmanager .trafficmanager.net

Routing method: Performance

Geographic routing

- When a Traffic Manager profile is configured for Geographic routing, each endpoint associated with that profile needs will have a set of geographic locations assigned to it. Any requests from those regions gets routed only to that endpoint. Some planning is required when you create a geographical endpoint. A location cannot be in more than one endpoint.

Geographic routing



Client connects **directly** to selected endpoint, **not** through Traffic Manager

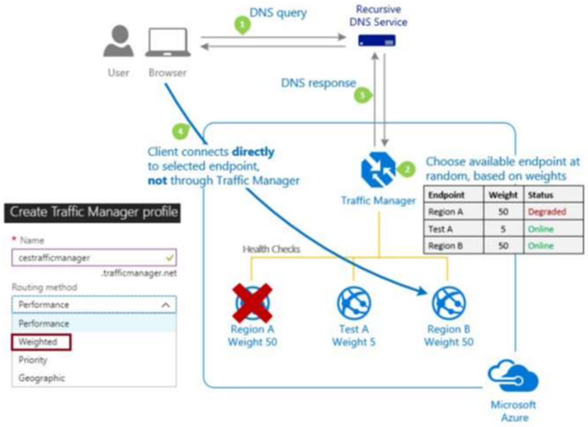
Choose the endpoint that is designated to serve the user's geographic region, based on the DNS query's source IP address

Endpoint	Assigned Geo
Endpoint 1	Germany
Nested Profile	Mexico, Asia
Endpoint 2	World

Weighted routing

- The Weighted traffic-routing method allows you to distribute traffic evenly or unevenly. In the Weighted traffic-routing method, you assign a weight to each endpoint in the Traffic Manager profile configuration. The weight is an integer from 1 to 1000. The higher weight, the higher the priority.

Weighted routing



Endpoint	Weight	Status
Region A	50	Degraded
Test A	5	Online
Region B	50	Online

Create Traffic Manager profile

* Name: cestrafficmanager ✓ .trafficmanager.net

Routing method: Performance

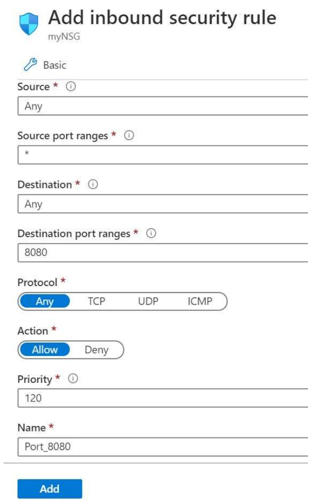
- Performance
- Weighted
- Priority
- Geographic

Network Security Groups

Network security groups filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

Network Security Groups (cont.)

- NSGs contain rules that specify whether traffic is approved or denied
- Each rule consists of the following properties:
  - Source
  - Source Port ranges
  - Destination
  - Destination port ranges
  - Protocol
  - Action
  - Priority
  - Name
- There are predefined default rules for inbound and outbound traffic



Add inbound security rule

myNSG

Basic

Source * Any

Source port ranges * *

Destination * Any

Destination port ranges * 8080

Protocol * [✓ Any] TCP UDP ICMP

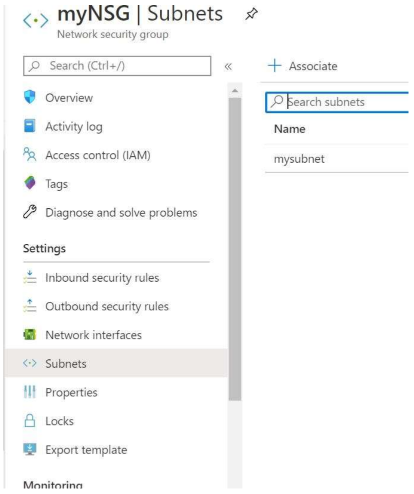
Action * [✓ Allow] Deny

Priority * 120

Name * Port_8080

Network Security Groups (cont.)

- Network security groups can be associated with a subnet or a network interface



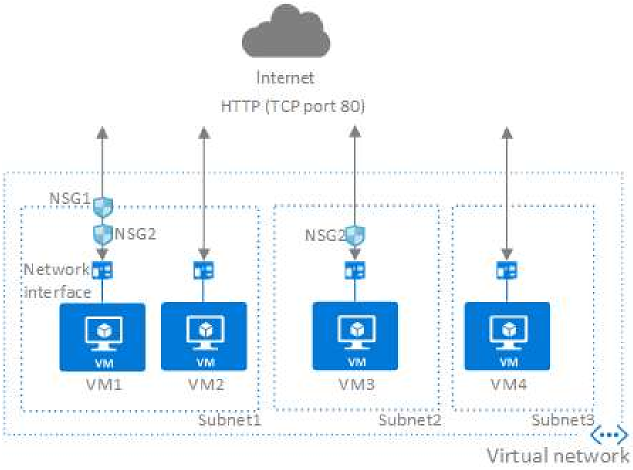
myNSG | Subnets

Network security group

Name
mysubnet

Network Security Groups (NSG)

- NSG1 allows port 80
- NSG2 allows port 3389
- NSG2 allows port 80

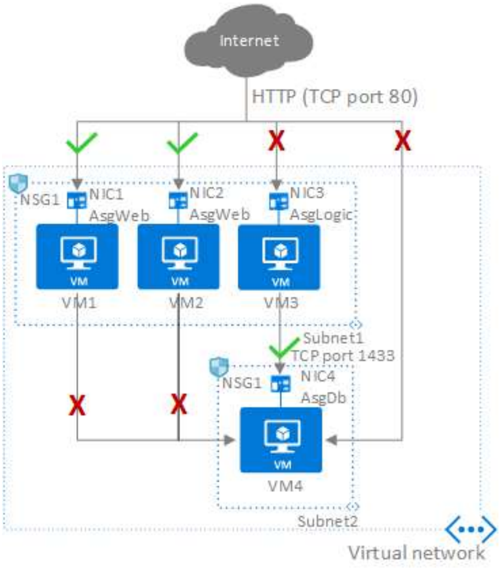


Application Security Groups

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

Application Security Groups

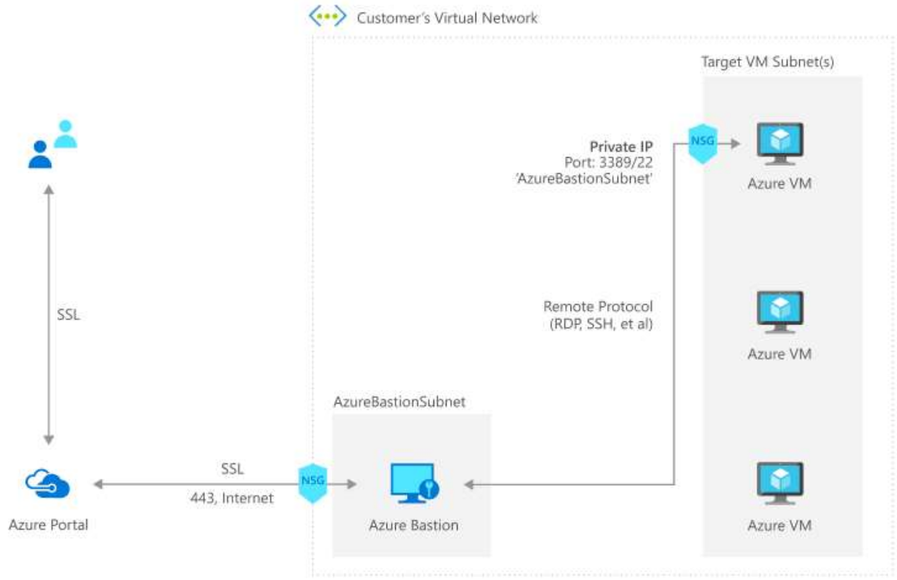
- NSG1 applies to subnet1 and subnet2
- AsgWeb applies to NIC1 and NIC2
- AsgLogic applies to NIC3
- AsgDb applies to NIC4

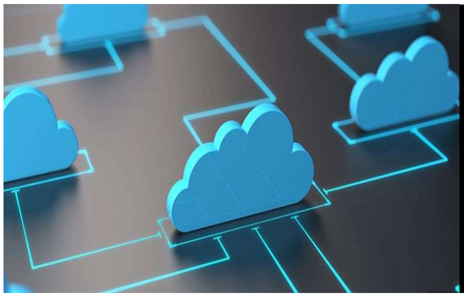


Azure Bastion

- Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP access to your virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in your Virtual Network (VNet) and supports all VMs in your Virtual Network (VNet) using SSL without any exposure through public IP addresses.

Azure Bastion





Module 6:
Azure Storage

Topics Covered

❑Understanding Azure Storage

❑Data Structure

❑Storage Tiers

❑Storage Services

❑Storage Account Types

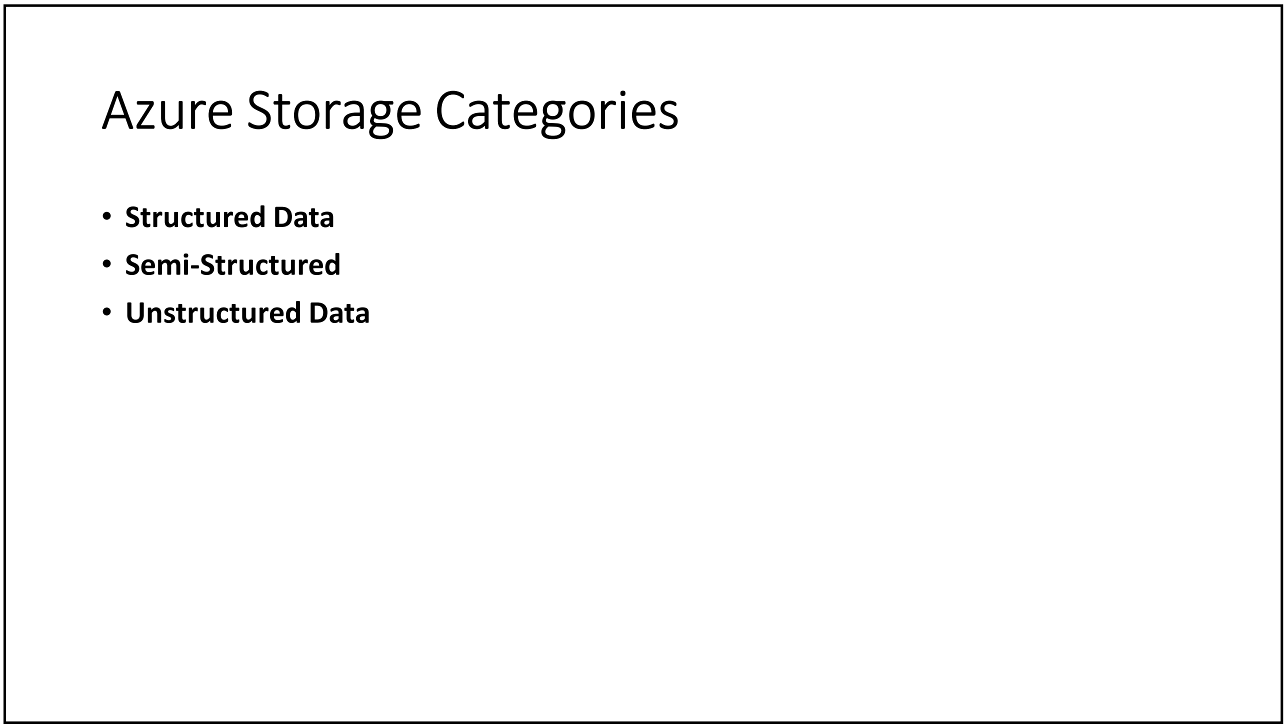
❑Data Redundancy

❑Storage Security

Azure Storage

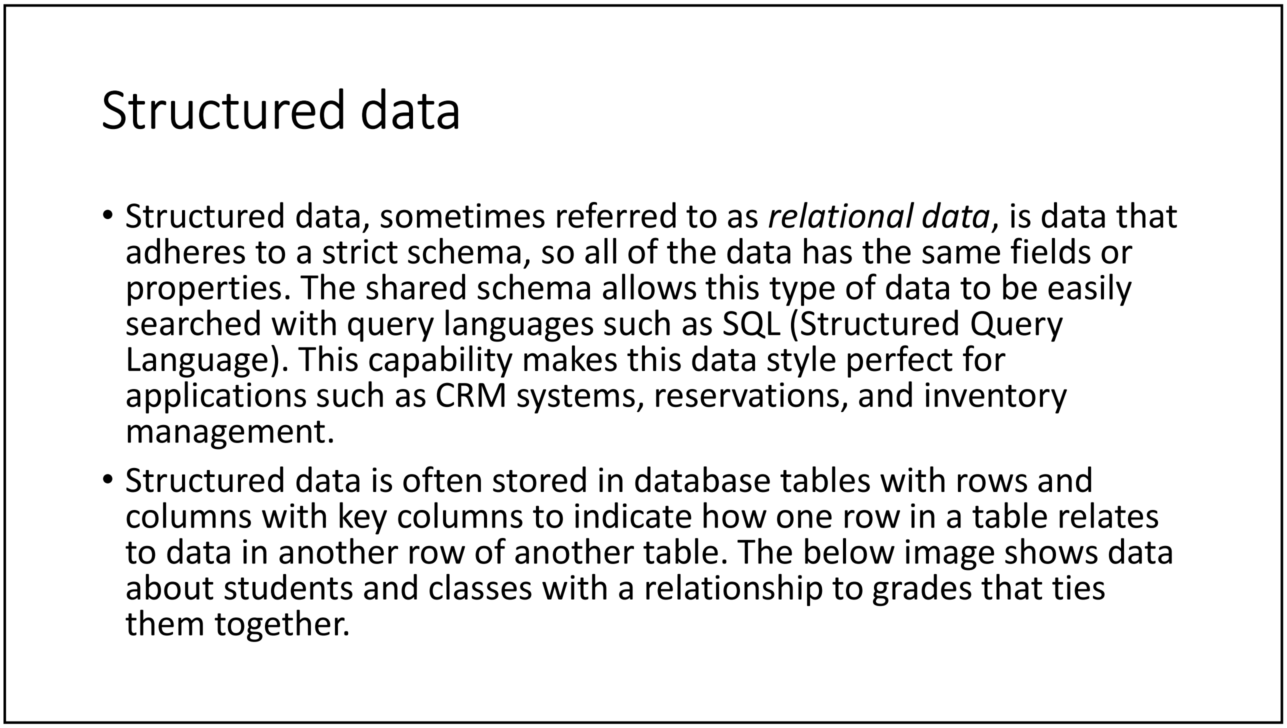
Azure Storage is Microsoft's cloud storage solution for modern data storage scenarios.

- **Durable and highly available**. Redundancy ensures that your data is safe in the event of hardware failures. You can also opt to replicate data across datacenters or geographical regions for additional protection from local catastrophe or natural disaster.
- **Secure**. All data written to Azure Storage is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.
- **Scalable**. Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- **Managed**. Microsoft Azure handles hardware maintenance, updates, and critical issues for you.
- **Accessible**. Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides SDKs for Azure Storage in a variety of languages – .NET, Java, Node.js, Python, PHP, Ruby, Go, and others – as well as a mature REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. The Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.



Azure Storage Categories

- **Structured Data**
- **Semi-Structured**
- **Unstructured Data**



Structured data

- Structured data, sometimes referred to as *relational data*, is data that adheres to a strict schema, so all of the data has the same fields or properties. The shared schema allows this type of data to be easily searched with query languages such as SQL (Structured Query Language). This capability makes this data style perfect for applications such as CRM systems, reservations, and inventory management.
- Structured data is often stored in database tables with rows and columns with key columns to indicate how one row in a table relates to data in another row of another table. The below image shows data about students and classes with a relationship to grades that ties them together.

Semi-structured data

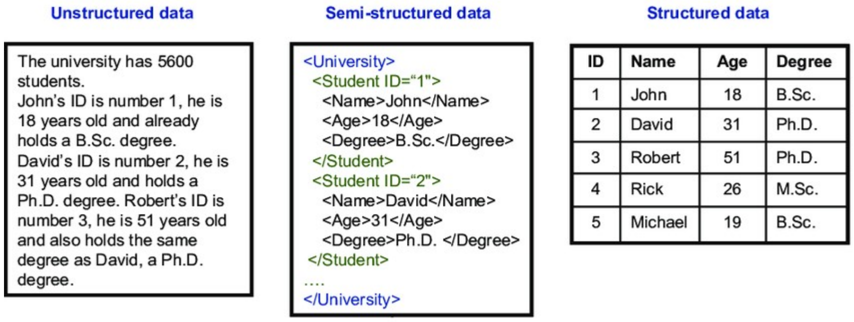
- Semi-structured data is less organized than structured data, and is not stored in a relational format, as the fields do not neatly fit into tables, rows, and columns. Semi-structured data contains tags that make the organization and hierarchy of the data apparent - for example, key/value pairs. Semi-structured data is also referred to as non-relational or *NoSQL data*.
- **JSON** is an type of semi-structured data

Unstructured data

The organization of unstructured data is ambiguous. Unstructured data is often delivered in files, such as photos or videos. Therefore, photos, videos, and other similar files are classified as unstructured data.

Examples of unstructured data include:

- Media files, such as photos, videos, and audio files
- Office files, such as Word documents
- Text files
- Log files



Unstructured data

The university has 5600 students.
John's ID is number 1, he is 18 years old and already holds a B.Sc. degree.
David's ID is number 2, he is 31 years old and holds a Ph.D. degree. Robert's ID is number 3, he is 51 years old and also holds the same degree as David, a Ph.D. degree.

Semi-structured data

```
<University>
 <Student ID="1">
  <Name>John</Name>
  <Age>18</Age>
  <Degree>B.Sc.</Degree>
 </Student>
 <Student ID="2">
  <Name>David</Name>
  <Age>31</Age>
  <Degree>Ph.D. </Degree>
</Student>
....
</University>
```

Structured data

ID	Name	Age	Degree
1	John	18	B.Sc.
2	David	31	Ph.D.
3	Robert	51	Ph.D.
4	Rick	26	M.Sc.
5	Michael	19	B.Sc.

Azure Storage Tiers

- **Standard** storage accounts are backed by magnetic drives (HDD) and provide the lowest cost per GB. They are best for applications that require bulk storage or where data is accessed infrequently.
- **Premium** storage accounts are backed by solid state drives (SSD) and offer consistent low-latency performance. They can only be used with Azure virtual machine disks and are best for I/O-intensive applications, like databases.

*Storage accounts can not be converted between standard and premium tiers

Azure Storage Services

- **Azure Containers (Blobs)**: A massively scalable object store for text and binary data.
- **Azure Files**: Managed file shares for cloud or on-premises deployments.
- **Azure Queues**: A messaging store for reliable messaging between application components.
- **Azure Tables**: A NoSQL store for schemaless storage of structured data.

Storage Account Types

- **General-purpose v1 accounts (Storage)**. Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.
- **General-purpose v2 accounts (StorageV2)**. Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.
- **Block blob storage accounts (BlockBlobStorage)**. Blob-only storage accounts with premium performance characteristics. Recommended for scenarios with high transactions rates, using smaller objects, or requiring consistently low storage latency.
- **FileStorage storage accounts (FileStorage)**. Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high performance scale applications.
- **Blob storage accounts (BlobStorage)**. Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

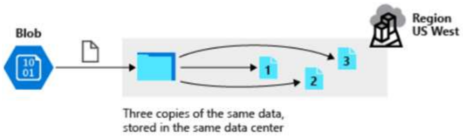
Data redundancy

Data in Azure is replicated to ensure that it's always available, even if a datacenter or region becomes inaccessible or a specific piece of hardware fails. You have four replication options:

- Locally redundant storage (LRS)
- Zone-redundant storage (ZRS)
- Geographically redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)

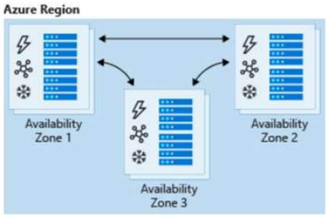
Locally redundant storage (LRS)

- Locally redundant storage replicates data and stores three copies across fault domains, or racks of hardware, within a single datacenter facility in one region. Data is replicated so that if there's a hardware fault or maintenance work, your data is still available and accessible.
- LRS protects your data from hardware failures, but you aren't protected if there's a datacenter outage.


Blob
10
01
1
2
3
Region
US West
Three copies of the same data,
stored in the same data center

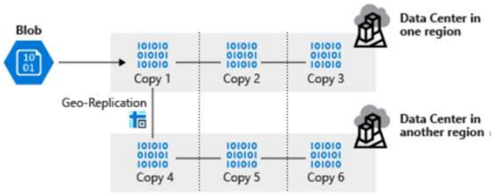
Zone-redundant storage (ZRS)

- Zone-redundant storage replicates your data across three storage clusters in a region. Each cluster is physically separated from the other two, which means that each cluster is supplied by separate utilities, such as power or networking.
- If there's an outage in a datacenter, you can still access your data from another availability zone in that region. Data is normally replicated to two or three availability zones, depending on the region.



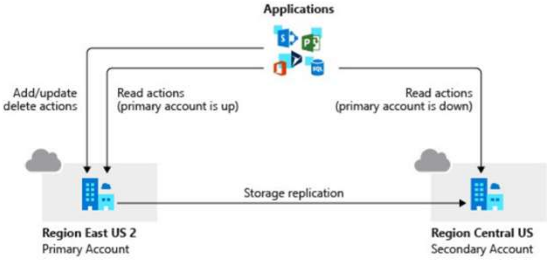
Geographically redundant storage (GRS)

- Geographically redundant, or geo-redundant, storage provides multiple levels of replication. Your data is replicated three times within the primary region, and then this set is replicated to a secondary region.



Read-access geo-redundant storage (RA-GRS)?

- Geo-redundant storage replicates data and objects to a secondary region. When failover starts, DNS entries that point to the primary region are updated to point to the secondary region. Microsoft currently controls the DNS failover process.
- When you use RA-GRS, you need to ensure that your application knows which endpoint it's interacting with. The secondary region has “-secondary” appended to the name of the endpoint.
- RA-GRS is ideal for applications, which require high availability.



Accessing Storage

Every object that you store in Azure Storage has a unique URL address. The storage account name forms the subdomain of that address. The combination of subdomain and domain name, which is specific to each service, forms an endpoint for your storage account.

If your storage account is named *mystorageaccount*, then the default endpoints for your storage account are:

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

The URL for accessing an object in a storage account is built by appending the object's location in the storage account to the endpoint.

For example, to access *myblob* in the *mycontainer*, use this format: http://mystorageaccount.blob.core.windows.net/mycontainer/myblob.

Storage Security

- **Encryption**. All data written to Azure Storage is automatically encrypted using Storage Service Encryption (SSE).
- **Authentication**. Azure Active Directory (Azure AD) and Role-Based Access Control (RBAC) are supported for Azure Storage for both resource management operations and data operations, as follows: You can assign RBAC roles scoped to the storage account to Users and Groups
- **Data in transit**. Data can be secured in transit between an application and Azure by using Client-Side Encryption, HTTPS, or SMB 3.0.
- **Disk encryption**. OS and data disks used by Azure virtual machines can be encrypted using Azure Disk Encryption.
- **Shared Access Signatures**. Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures.

Data Box

Data Box Disk (40 TB)
- Supports Azure Blobs, Files and Managed Disks
- Copy data to 1 storage account
- USB 3.1/SATA interface

Data Box (100 TB)
- Supports Azure Blobs, Files and Managed Disks
- Copy data across 10 storage accounts
- 1x10 Gbps RJ45, 2x10 Gbps SFP+ interface

Data Box Heavy (1000 TB)
- Supports Azure Blobs, Files and Managed Disks
- Copy data across 10 storage accounts
- 4x1 Gbps, 4x40 Gbps interface

Send your own disks 1TB

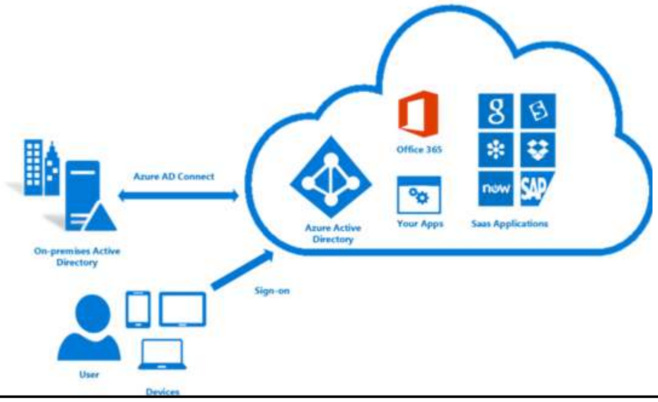
Module 7:
Identity Management

Topics Covered

- □Understanding Identity Management
- □Managing Users and Groups
- □Multi-Factor Authentication
- □Conditional Access
- □Password Management
- □Domain Names

Identity Management

On-premises Active Directory, Azure AD, or a hybrid combination of the two all offer services for user and device authentication, identity and role management, and provisioning



Understand users and groups

- In Azure AD, every user who needs access to resources requires a user account
- Azure AD defines users in three ways:
  - Cloud identities
  - Directory-synchronized identities
  - Guest users
- You can add cloud identities to Azure AD by using:
  - Azure portal
  - Azure PowerShell

Configuring Multi-Factor Authentication (MFA)

Azure AD

- Security Defaults
- MFA Configuration
- Enable MFA

What is Multi-Factor Authentication (MFA)?

- Azure MFA is the multi-step verification solution from Microsoft
- Azure MFA supplies added security for your identities by requiring two or more elements for full authentication
- These elements fall into three categories:
  - **Something you know**: password or answer to security question
  - **Something you possess**: mobile app or token device
  - **Something you are**: biometric property such as fingerprint
- Using Azure MFA increases identity security by limiting the impact of credential exposure

Multi-Factor Authentication Offerings

Azure MFA comes as part of the following offerings:

- Azure Active Directory Premium licenses
  - Azure MFA Service (Cloud)
  - Azure MFA Server (on premise)
- Multi-Factor Authentication for Microsoft Office 365

Configure Trusted IPs

Azure AD enables single sign-on to devices, apps, and services from anywhere on the public internet. With the location condition, you can control access to your cloud apps based on the network location of a user. Common use cases for the location condition are:

- Requiring multi-factor authentication for users accessing a service when they are off the corporate network.
- Blocking access for users accessing a service from specific countries or regions.

A location is a label for a network location that either represents a named location or multi-factor authentication Trusted IPs.

Domain Names

Initial domain name

- By default, when you create an Azure subscription an Azure AD domain is created for you. This instance of the domain has *initial domain name* in the form *domainname.onmicrosoft.com*. The initial domain name, while fully functional, is intended primarily to be used as a bootstrapping mechanism until a custom domain name is verified.

Custom domain name

- Although the initial domain name for a directory can't be changed or deleted, you can add any routable custom domain name you control. This simplifies the user sign-on experience by allowing user to logon with credentials they are familiar with. For example, a contosogold.onmicrosoft.com, could be assigned a simpler custom domain name of contosogold.com.

Domain name administration

- Only a global administrator can perform domain management tasks in Azure AD, by default this is the user who created the subscription.
- Domain names in Azure AD are globally unique. If one Azure AD directory has verified a domain name, then no other Azure AD directory can verify or use that same domain name.
- Before a custom domain name can be used by Azure AD, the custom domain name must be added to your directory and verified. This is covered in the next topic.

Verifying Custom Domain Names

- When an administrator adds a custom domain name to an Azure AD, it is initially in an unverified state. Azure AD will not allow any directory resources to use an unverified domain name. This ensures that the organization using the domain name owns that domain name.
- After adding the custom domain name, you must verify ownership of the domain name, this is done by adding a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone. Once this record is added, Azure will query the DNS domain for the presence of the record. This could take several minutes or several hours. If Azure verifies the presence of the DNS record, it will then add the domain name to the subscription.

Module 8:
Azure Roles, Policies and Blueprints

Topics Covered

❑Understanding Role Based Access Control (RBAC)

❑Azure Policies

❑Azure Blueprints

Role-Based Access Control (RBAC)

- Role-based access control (RBAC) is an authorization system built on Azure Resource Manager that provides fine-grained access management of resources in Azure. With RBAC, you can grant the exact access that users need to do their jobs.
- You grant access by assigning the appropriate RBAC role to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource. A role assigned at a parent scope also grants access to the child scopes contained within it.

Azure roles and Azure AD roles

Azure roles control permissions to manage Azure resources, while Azure AD roles control permissions to manage Azure Active Directory resources. The following table compares some of the differences.

- **Access control (IAM)** is the blade that you use to assign roles to grant access to Azure resources
- **Roles and Administrators** is used to grant access to Azure AD and other Microsoft services

Understanding Azure Policy

- Azure Policy helps to enforce organizational standards and to assess compliance. Through its compliance dashboard, it provides a view to evaluate the overall state of the environment.
- Azure Policy also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Azure Blueprints

- Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
- The Azure Blueprints service is designed to help with environment setup, which often consists of a set of resource groups, policies, role assignments, and Resource Manager template deployments. A blueprint is a package to bring each of these artifact types together

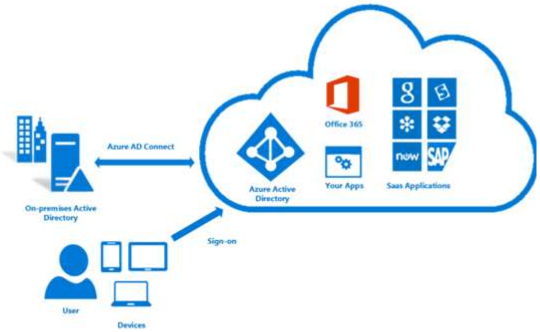
Module 9:
Azure AD

Topics Covered

- □Hybrid Identity in Azure
- □Azure AD Connect
- □Configure Sync Features

Hybrid Identity with Azure Active Directory

- Organizations are a mixture of on-premises and cloud applications. Users require access to those applications both on-premises and in the cloud.
- Microsoft’s identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.



Azure AD Connect

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It provides the following features:

- **Password hash synchronization** - A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.
- **Pass-through authentication** - A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.
- **Federation integration** - Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- **Synchronization** - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
- **Health Monitoring** - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Azure AD Connect Installation

- **Azure AD Connect Express Settings** is used when you have a single-forest topology and password hash synchronization for authentication. Express Settings is the default option and is used for the most commonly deployed scenario.
- **Azure AD Connect Custom** settings is used when you want more options for the installation. It is used if you have multiple forests or if you want to configure optional features not covered in the express installation. It is used in all cases where the express installation option does not satisfy your deployment or topology.

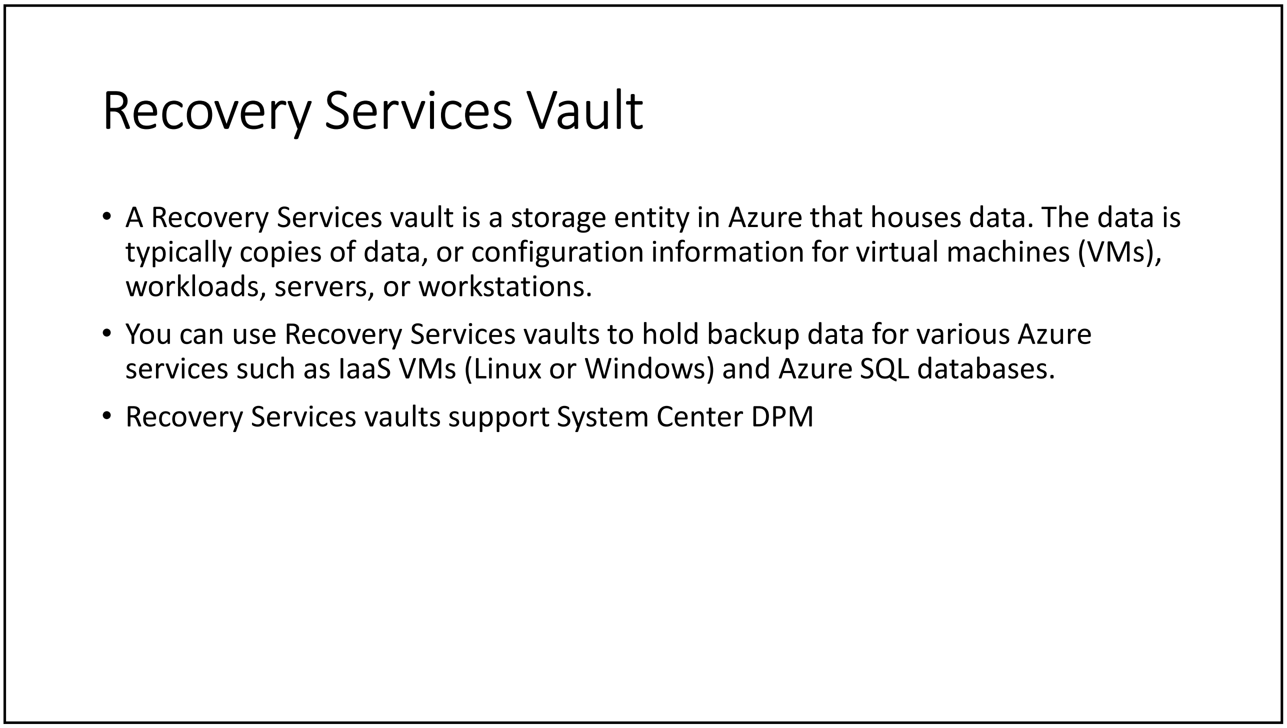
Configure sync features

- **Filtering** is used when you want to limit which objects are synchronized to Azure AD. By default all users, contacts, groups, and Windows 10 computers are synchronized. You can change the filtering based on domains, OUs, or attributes.
- **Password hash synchronization** synchronizes the password hash in Active Directory to Azure AD. The end-user can use the same password on-premises and in the cloud but only manage it in one location. Since it uses your on-premises Active Directory as the authority, you can also use your own password policy.
- **Password writeback** allows your users to change and reset their passwords in the cloud and have your on-premises password policy applied.
- **Device writeback** allows a device registered in Azure AD to be written back to on-premises Active Directory so it can be used for Conditional Access.
- The **prevent accidental deletes** feature is turned on by default and protects your cloud directory from numerous deletes at the same time. By default it allows 500 deletes per run. You can change this setting depending on your organization size.
- **Automatic upgrade** is enabled by default for express settings installations and ensures your Azure AD Connect is always up to date with the latest release.

Module 10:
Azure Backup and Recovery

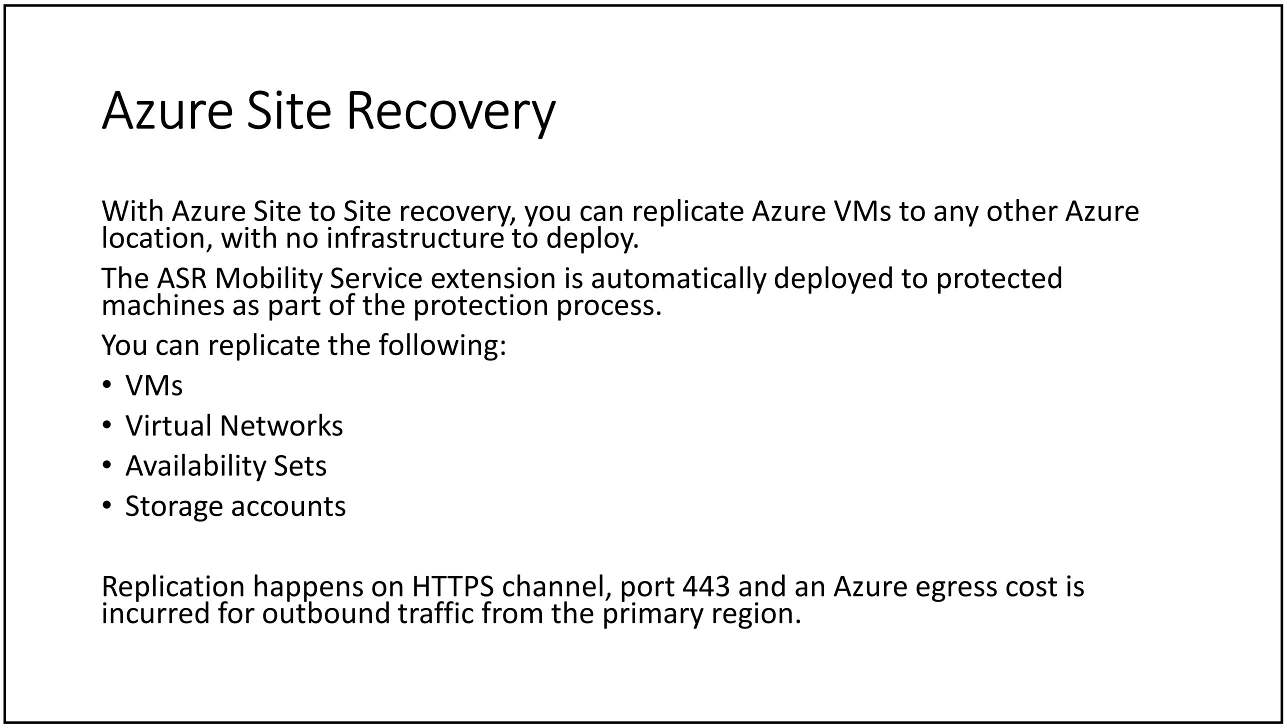
Topics Covered

□Azure Recovery Services Vault
□Azure Site Recovery
□Azure Backup
□Update Management



Recovery Services Vault

- A Recovery Services vault is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations.
- You can use Recovery Services vaults to hold backup data for various Azure services such as IaaS VMs (Linux or Windows) and Azure SQL databases.
- Recovery Services vaults support System Center DPM



Azure Site Recovery

With Azure Site to Site recovery, you can replicate Azure VMs to any other Azure location, with no infrastructure to deploy.

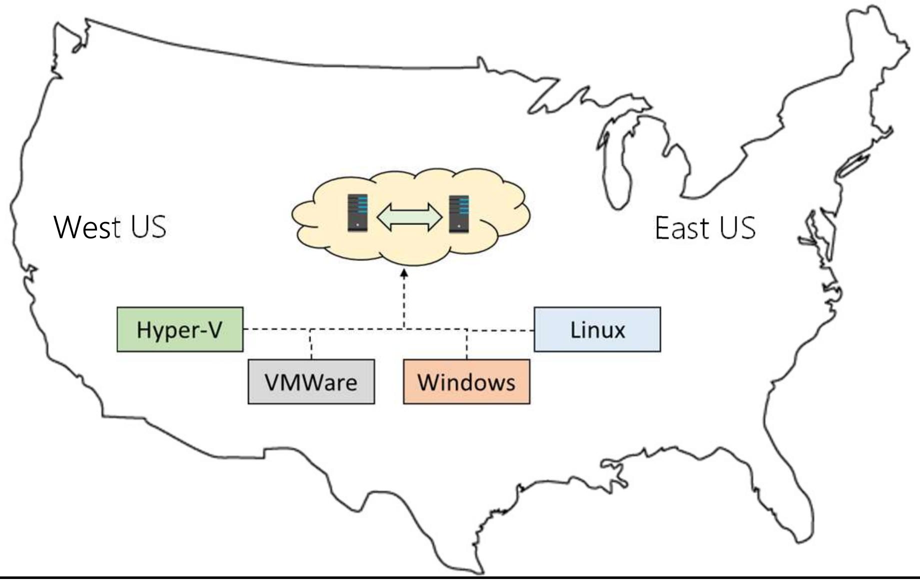
The ASR Mobility Service extension is automatically deployed to protected machines as part of the protection process.

You can replicate the following:

- VMs
- Virtual Networks
- Availability Sets
- Storage accounts

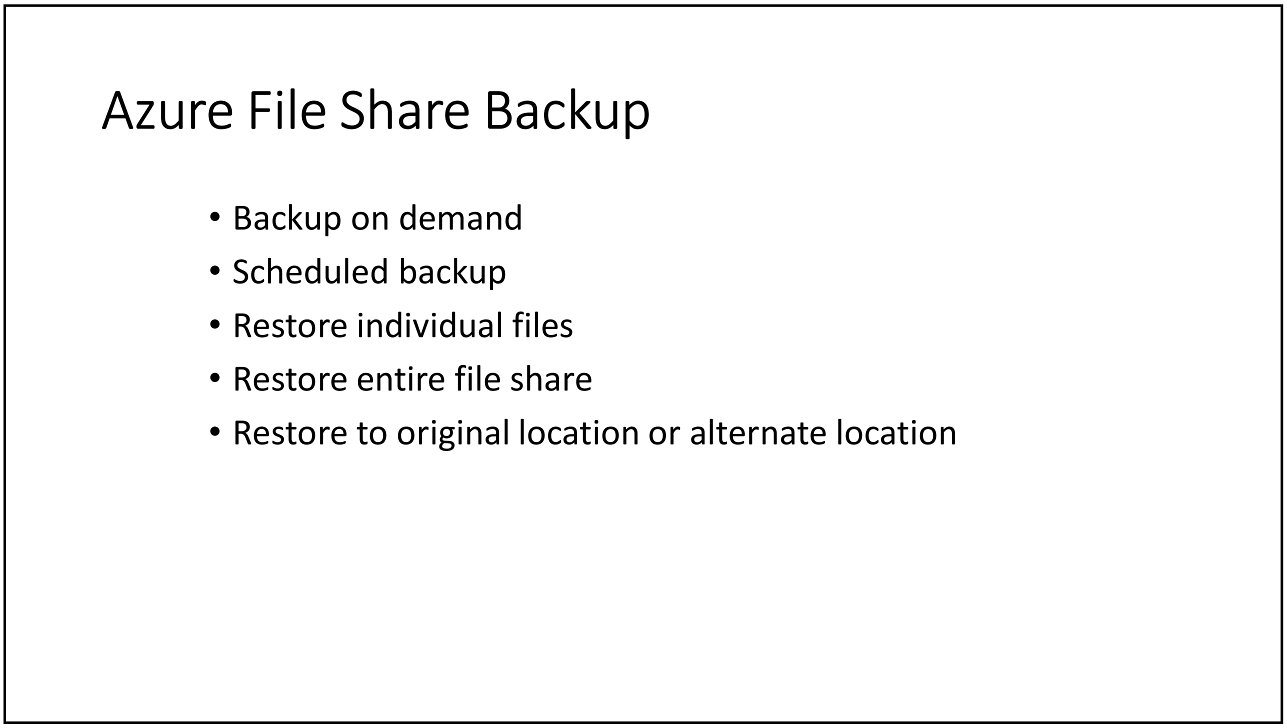
Replication happens on HTTPS channel, port 443 and an Azure egress cost is incurred for outbound traffic from the primary region.

Azure Site Recovery



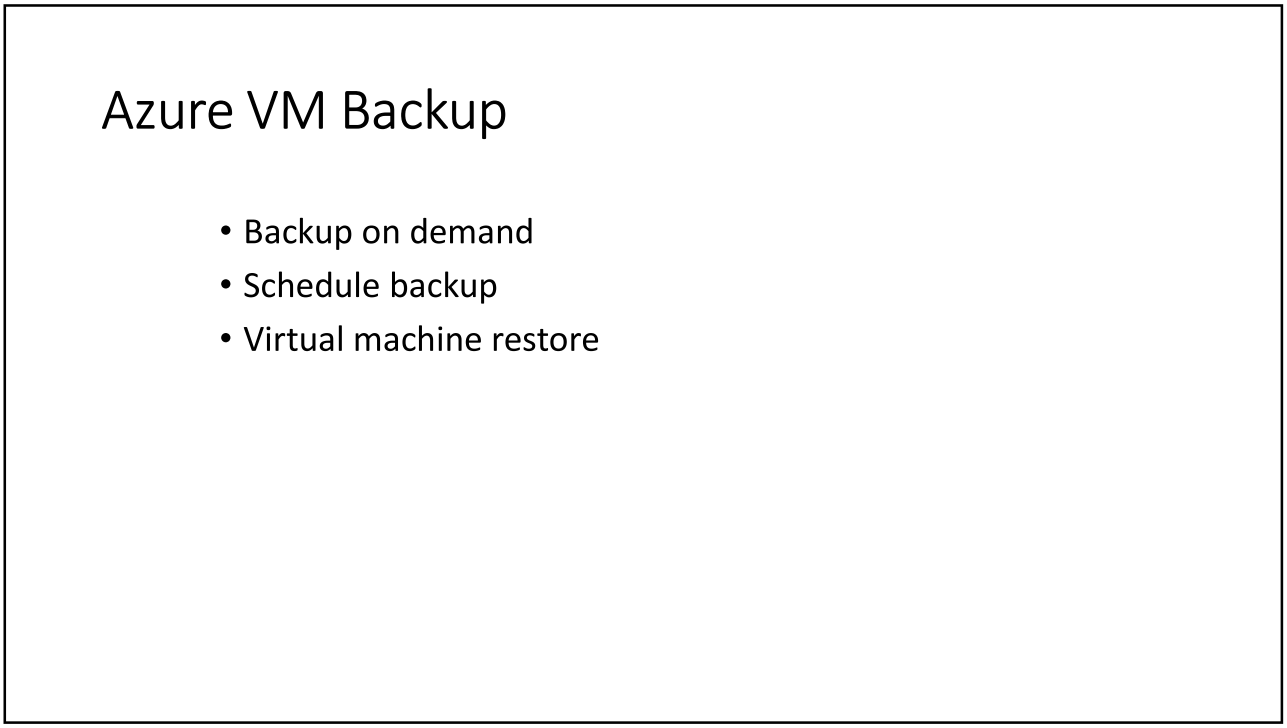
Azure Backup

- Offload on-premise backup
- Backup Azure VMs
- Unlimited data transfer
- Data security
- Locally redundant storage (LRS) or geo-redundant storage of backups (GRS)



Azure File Share Backup

- Backup on demand
- Scheduled backup
- Restore individual files
- Restore entire file share
- Restore to original location or alternate location



Azure VM Backup

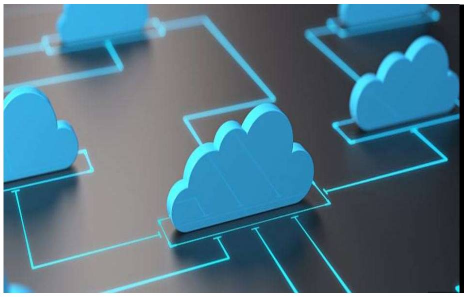
- Backup on demand
- Schedule backup
- Virtual machine restore

On-premise backup to Azure

- Download and Install MARS agent
  - Files and Folders
  - Hyper-V virtual machines
  - Vmware virtual machines
  - SQL Servers
  - SharePoint Servers
  - Exchange Servers
  - System State
  - Bare Metal Recovery

Update Management

- You can use the Update Management solution in Azure Automation to manage operating system updates:
- For computers running the Windows and Linux operating systems.
- For computers deployed in Azure.
- In on-premises environments.
- In other cloud providers.



Module 11:
Monitoring Azure Resources and Services

Topics Covered

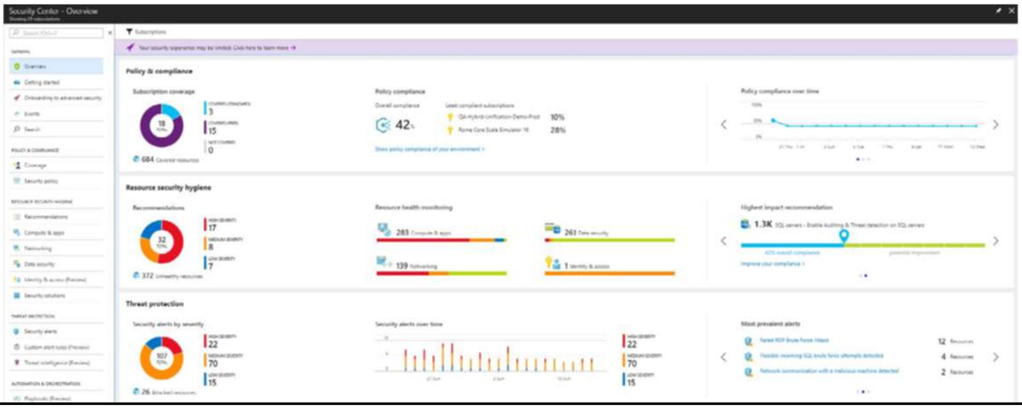
❑Azure Security Center

❑Azure Monitor

❑Azure Advisor

Azure Security Center

- Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.



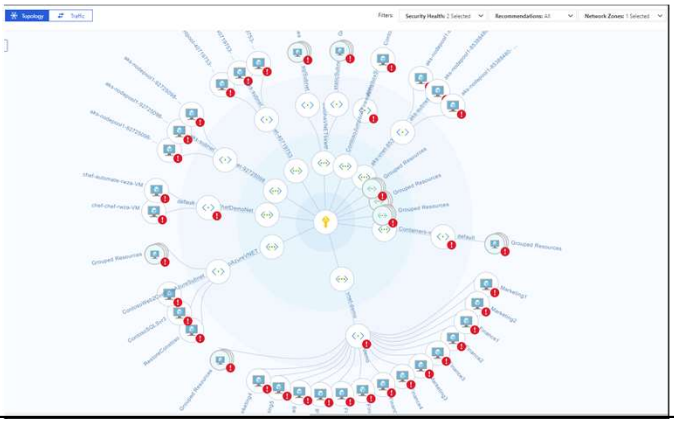
Azure Security Center

Azure Security Center addresses the three most urgent security challenges:

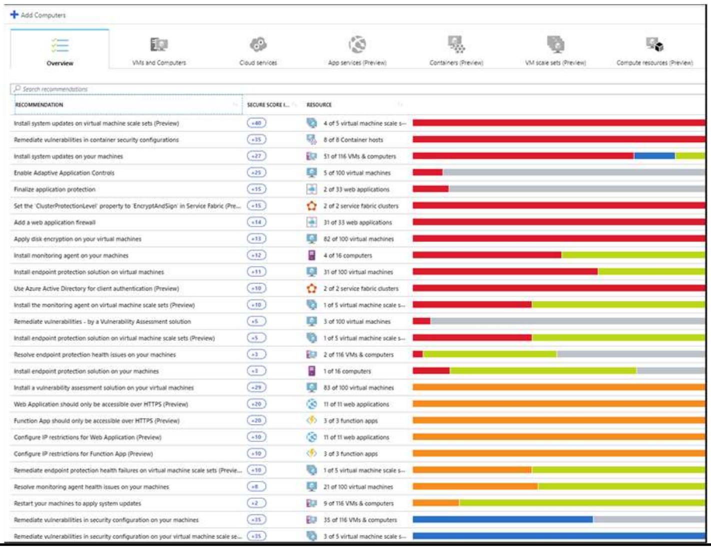
- **Rapidly changing workloads** – It's both a strength and a challenge of the cloud. On the one hand, end users are empowered to do more. On the other, how do you make sure that the ever-changing services people are using and creating are up to your security standards and follow security best practices?
- **Increasingly sophisticated attacks** - Wherever you run your workloads, the attacks keep getting more sophisticated. You have to secure your public cloud workloads, which are, in effect, an Internet facing workload that can leave you even more vulnerable if you don't follow security best practices.
- **Security skills are in short supply** - The number of security alerts and alerting systems far outnumbers the number of administrators with the necessary background and experience to make sure your environments are protected. Staying up-to-date with the latest attacks is a constant challenge, making it impossible to stay in place while the world of security is an ever-changing front.

Network Map

The network map enables you to see the topology of your workloads, so you can see if each node is properly configured. You can see how your nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along your network.

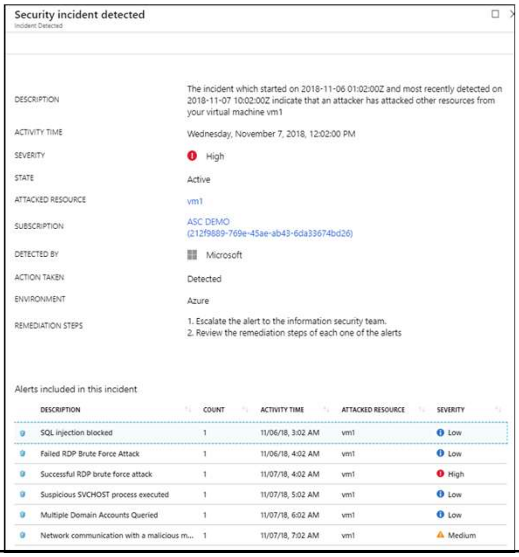


Protect against threats



RECOMMENDATION	SECURE SCORE I...	RESOURCE
Install system updates on virtual machine scale sets (Preview)	+40	4 of 5 virtual machine scale s...
Remediate vulnerabilities in container security configurations	+35	8 of 8 Container hosts
Install system updates on your machines	+27	51 of 116 VMs & computers
Enable Adaptive Application Controls	+25	5 of 100 virtual machines
Finalize application protection	+15	2 of 33 web applications
Set the 'ClusterProtectionLevel' property to 'EncryptAndSign' in Service Fabric (Pre...	+15	2 of 2 service fabric clusters
Add a web application firewall	+14	31 of 33 web applications
Apply disk encryption on your virtual machines	+13	82 of 100 virtual machines
Install monitoring agent on your machines	+12	4 of 16 computers
Install endpoint protection solution on virtual machines	+11	31 of 100 virtual machines
Use Azure Active Directory for client authentication (Preview)	+10	2 of 2 service fabric clusters
Install the monitoring agent on virtual machine scale sets (Preview)	+10	1 of 5 virtual machine scale s...
Remediate vulnerabilities - by a Vulnerability Assessment solution	+5	3 of 100 virtual machines
Install endpoint protection solution on virtual machine scale sets (Preview)	+5	1 of 5 virtual machine scale s...
Resolve endpoint protection health issues on your machines	+3	2 of 116 VMs & computers
Install endpoint protection solution on your machines	+3	1 of 16 computers
Install a vulnerability assessment solution on your virtual machines	+29	83 of 100 virtual machines
Web Application should only be accessible over HTTPS (Preview)	+20	11 of 11 web applications
Function App should only be accessible over HTTPS (Preview)	+20	3 of 3 function apps
Configure IP restrictions for Web Application (Preview)	+10	11 of 11 web applications
Configure IP restrictions for Function App (Preview)	+10	3 of 3 function apps
Remediate endpoint protection health failures on virtual machine scale sets (Previe...	+10	1 of 5 virtual machine scale s...
Resolve monitoring agent health issues on your machines	+8	21 of 100 virtual machines
Restart your machines to apply system updates	+2	9 of 116 VMs & computers
Remediate vulnerabilities in security configuration on your machines	+35	35 of 116 VMs & computers
Remediate vulnerabilities in security configuration on your virtual machine scale se...	+35	3 of 5 virtual machine scale s...

Block Brute Force Attacks



Security incident detected
Incident Detected

DESCRIPTION	The incident which started on 2018-11-06 01:02:00Z and most recently detected on 2018-11-07 10:02:00Z indicate that an attacker has attacked other resources from your virtual machine vm1
ACTIVITY TIME	Wednesday, November 7, 2018, 12:02:00 PM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	vm1
SUBSCRIPTION	ASC DEMO (212f9889-769e-45ae-ab43-6da33674bd26)
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
REMEDIATION STEPS	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts

Alerts included in this incident

DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY
SQL injection blocked	1	11/06/18, 3:02 AM	vm1	Low
Failed RDP Brute Force Attack	1	11/06/18, 4:02 AM	vm1	Low
Successful RDP brute force attack	1	11/07/18, 4:02 AM	vm1	High
Suspicious SVCHOST process executed	1	11/07/18, 5:02 AM	vm1	Low
Multiple Domain Accounts Queried	1	11/07/18, 6:02 AM	vm1	Low
Network communication with a malicious m...	1	11/07/18, 7:02 AM	vm1	Medium

Azure Monitor

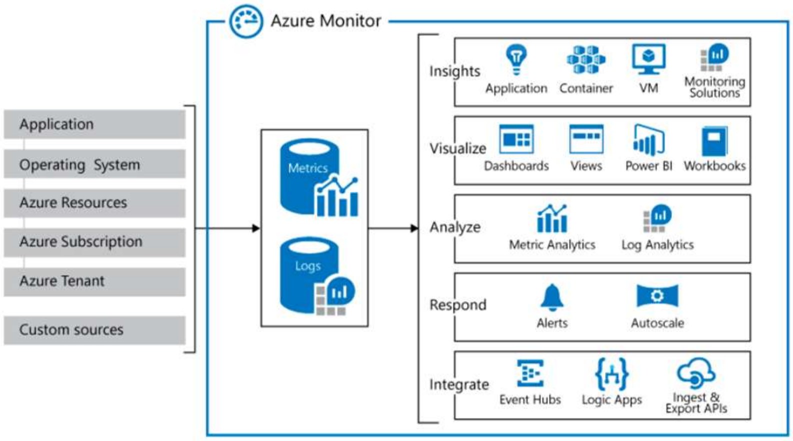
Azure Monitor maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

What data does Azure Monitor collect?

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

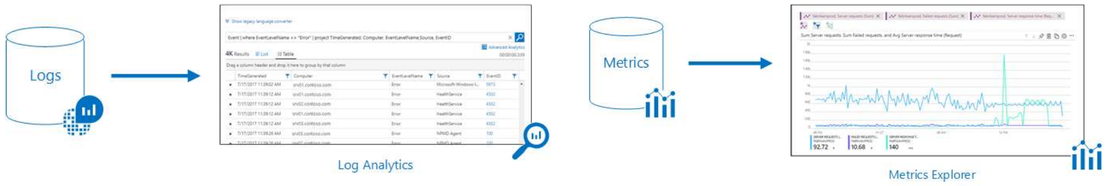
- **Application monitoring data**: Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data**: Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data**: Data about the operation of an Azure resource.
- **Azure subscription monitoring data**: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data**: Data about the operation of tenant-level Azure services, such as Azure Active Directory.

Azure Monitor



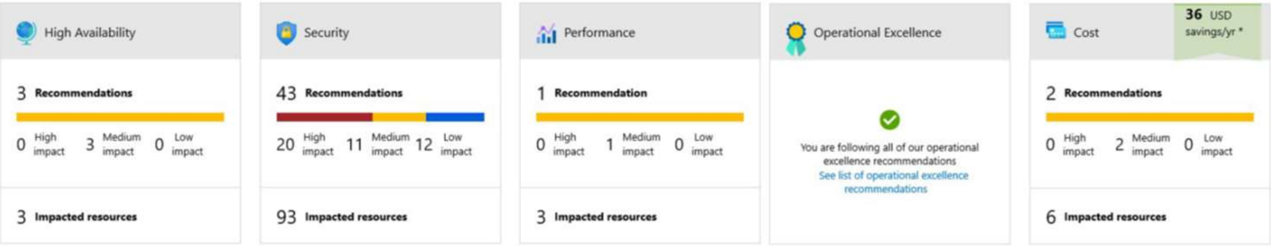
Monitoring data platform

- All data collected by Azure Monitor fits into one of two fundamental types, metrics and logs.
- ***Metrics*** are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios.
- ***Logs*** contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.



Azure Advisor

- Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.
- The Advisor cost recommendations page helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources.



High Availability

3 Recommendations

0 High impact 3 Medium impact 0 Low impact

3 Impacted resources

Security

43 Recommendations

20 High impact 11 Medium impact 12 Low impact

93 Impacted resources

Performance

1 Recommendation

0 High impact 1 Medium impact 0 Low impact

3 Impacted resources

Operational Excellence

You are following all of our operational excellence recommendations

See list of operational excellence recommendations

Cost

36 USD savings/yr *

2 Recommendations

0 High impact 2 Medium impact 0 Low impact

6 Impacted resources

Module 12:
Azure Key Vault

Topics Covered

- □Azure Key Vault Overview
- □Vault Isolation
- □User Assignment

Understanding the Azure Key Vault

- Azure Key Vault helps safeguard cryptographic keys and secrets that cloud applications and services use.
- Key Vault simplifies the key management process and enables you to control keys that access and encrypt your data.

Example: An application stores social security numbers for employees. Azure Key Vault allows you to encrypt the social security numbers. This could be used for any PII or sensitive data.

- Security administrators can grant and revoke permission to keys at anytime.

Benefits of using the Azure Key Vault

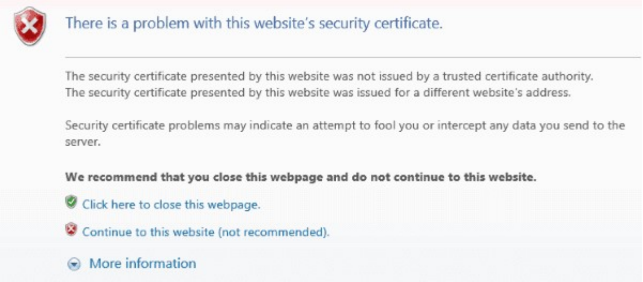
- **Secrets management**. Azure Key Vault can securely store and control access to passwords, certificates and other secrets.

- **Key management**. Azure Key Vault is a cloud-based key management solution, making it easier to create and control the encryption keys used to encrypt your data. Azure services such as App Service integrate directly with Azure Key Vault.

What can I use the Azure Key Vault for?

- **Certificate management**. Azure Key Vault is also a service that lets you provision, manage, and deploy public and private SSL/TLS certificates for use with Azure and your internal resources.

It can also request and renew TLS certificates with certificate authorities (CAs)



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

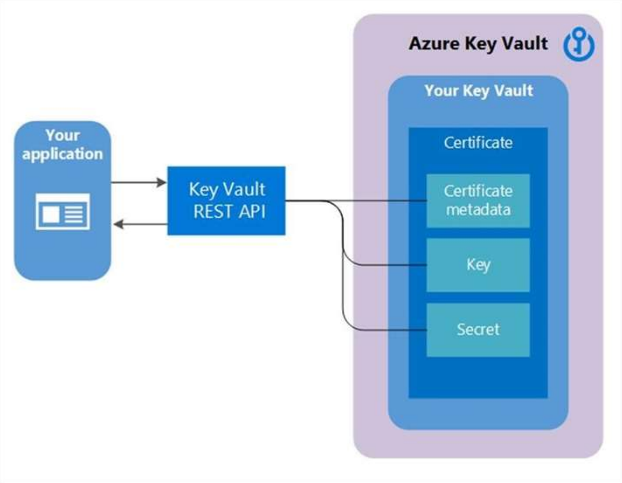
Click here to close this webpage.

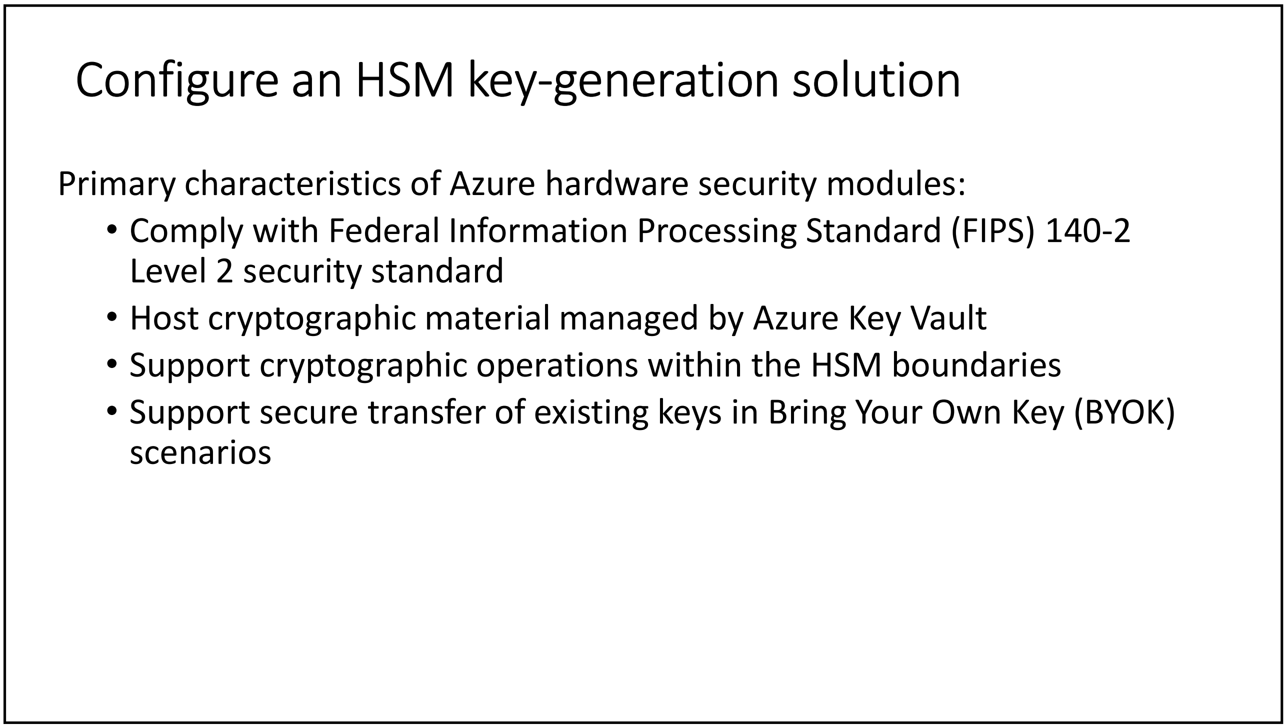
Continue to this website (not recommended).

More information

Manage certificates

- Create certificates
- Secure storage for certificates
- Audit and notifications
- Automatic renewal

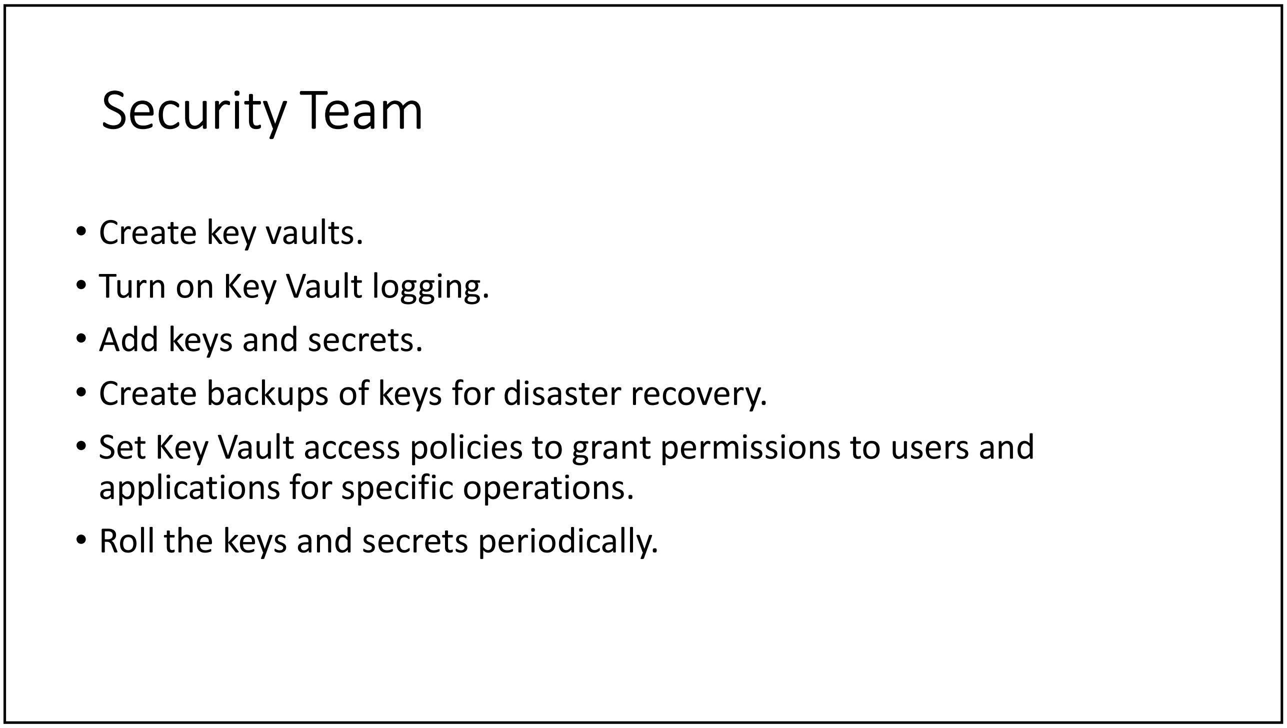




Configure an HSM key-generation solution

Primary characteristics of Azure hardware security modules:

- Comply with Federal Information Processing Standard (FIPS) 140-2 Level 2 security standard
- Host cryptographic material managed by Azure Key Vault
- Support cryptographic operations within the HSM boundaries
- Support secure transfer of existing keys in Bring Your Own Key (BYOK) scenarios



Security Team

- Create key vaults.
- Turn on Key Vault logging.
- Add keys and secrets.
- Create backups of keys for disaster recovery.
- Set Key Vault access policies to grant permissions to users and applications for specific operations.
- Roll the keys and secrets periodically.

Developers and Operators

- Get references from the security team for the bootstrap and SSL certificates (thumbprints), storage key (secret URI), and RSA key (key URI) for signing.
- Develop and deploy the application to access keys and secrets programmatically.

Auditors

- Review the Key Vault logs to confirm proper use of keys and secrets, and compliance with data security standards.

Module 13:
Azure Applications

Topics Covered

- □Understanding the Azure App Service
- □Deployment Slots
- □App Service Plans
- □Implementing Logic Apps
- □Implementing Azure Functions

Create and Configure Azure App Service

- Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. You can develop in your favorite language, be it .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. Applications run and scale with ease on both Windows and Linux-based environments.
- App Service not only adds the power of Microsoft Azure to your application, such as security, load balancing, autoscaling, and automated management. App Service also supports custom domains, and TLS/SSL certificates.
- With App Service, you pay for the Azure compute resources you use. The compute resources

Deployment slots

- Using the Azure portal, you can easily add **deployment slots** to an App Service web app. For instance, you can create a **staging** deployment slot where you can push your code to test on Azure. Once you are happy with your code, you can easily **swap** the staging deployment slot with the production slot. You do all this with a few simple mouse clicks in the Azure portal.

Implement Logic Apps

Azure Logic Apps is a cloud service that helps you schedule, automate, and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations. For example, here are just a few workloads you can automate with logic apps:

- Process and route orders across on-premises systems and cloud services.
- Send email notifications with Office 365 when events happen in various systems, apps, and services.
- Move uploaded files from an SFTP or FTP server to Azure Storage.
- Monitor tweets for a specific subject, analyze the sentiment, and create alerts or tasks for items that need review.

Implement Azure Functions

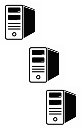
- Azure Functions is serverless computing, which allows you to run small pieces of code (called “functions”) without worrying about application infrastructure. With Azure Functions, the cloud infrastructure provides all the up-to-date servers you need to keep your application running at scale.
- Applications can be C#, Node.js, Java, .Net or Python
- A function is “triggered” by a specific type of event. Supported triggers include responding to changes in data, responding to messages, running on a schedule, or as the result of an HTTP request.

Module 14:
Containers and Kubernetes

Topics Covered

❑Containers
❑Docker
❑Kubernetes

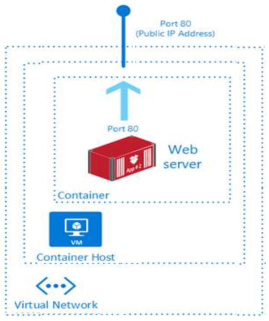
Containers vs Virtual Machines



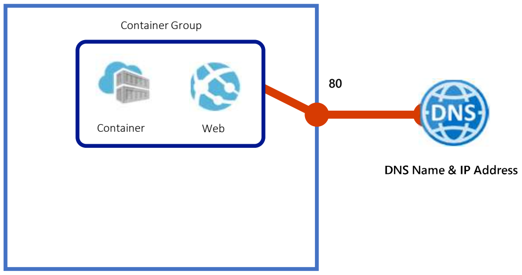
Feature	Containers	Virtual Machines
Isolation	Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.	Provides complete isolation from the host operating system and other VMs. This is useful when a strong security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

Azure Container Instances

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



Container Groups



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

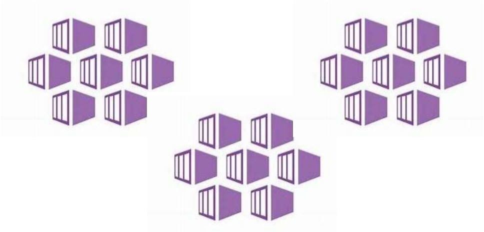
Docker

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

https://hub.docker.com/

Kubernetes core concepts for Azure Kubernetes Service (AKS)

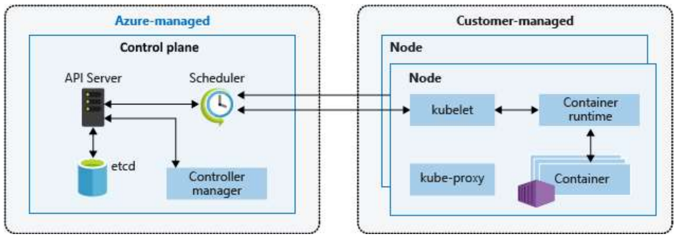
As application development moves towards a container-based approach, the need to orchestrate and manage resources is important. Kubernetes is the leading platform that provides the ability to provide reliable scheduling of fault-tolerant application workloads. Azure Kubernetes Service (AKS) is a managed Kubernetes offering that further simplifies container-based application deployment and management.



What is Kubernetes?

- Kubernetes is a rapidly evolving platform that manages container-based applications and their associated networking and storage components. The focus is on the application workloads, not the underlying infrastructure components.
- You can build and run modern, portable, microservices-based applications that benefit from Kubernetes and manage the availability of those application components.
- As an open platform, Kubernetes allows you to build your applications with your preferred programming language.
- The AKS control plane is managed by the Azure platform, and you only pay for the AKS nodes that run your applications. AKS is built on top of the open-source Azure Kubernetes Service Engine

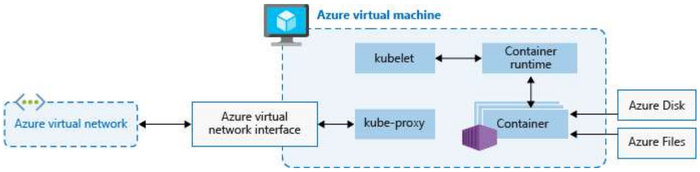
Kubernetes Cluster Architecture



The control plane includes the following core Kubernetes components:

- *kube-apiserver* - The API server is how the underlying Kubernetes APIs are exposed. This component provides the interaction for management tools, such as the Kubernetes dashboard.
- *etcd* - To maintain the state of your Kubernetes cluster and configuration, the highly available *etcd* is a key value store within Kubernetes.
- *kube-scheduler* - When you create or scale applications, the Scheduler determines what nodes can run the workload and starts them.
- *kube-controller-manager* - The Controller Manager oversees a number of smaller Controllers that perform actions such as replicating pods and handling node operations.

Kubernetes Cluster Architecture



- To run your applications and supporting services, you need a Kubernetes *node*. An AKS cluster has one or more nodes, which is an Azure virtual machine (VM) that runs the Kubernetes node components and container runtime:
- The kubelet is the Kubernetes agent that processes the requests from the control plane and scheduling of running the requested containers.
- Virtual networking is handled by the *kube-proxy* on each node. The proxy routes network traffic and manages IP addressing for services and pods.
- The *container runtime* is the component that allows containerized applications to run and interact with additional resources such as the virtual network and storage. In AKS, Moby is used as the container runtime.

- INTENTIONALLY LEFT BLANK

Database Exams and Certifications

- DP-900: Microsoft Azure Data Fundamentals
- 70-777: Implementing Microsoft Azure Cosmos DB Solutions
- DP-100: Designing and Implementing a Data Science Solution on Azure
- DP-200, DP-201: Microsoft Certified: Azure Data Engineer Associate
- DP-300: Microsoft Certified: Azure Database Administrator Associate
- AZ-220: Microsoft Azure IoT Developer

- INTENTIONALLY LEFT BLANK

Module 15: Azure NoSQL and Cosmos DB

Topics Covered

❑Azure NoSQL

❑Azure Cosmos DB

Implement NoSQL Databases

- Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schemaless design. Because Table storage is schemaless, it's easy to adapt your data as the needs of your application evolve. Access to Table storage data is fast and cost-effective for many types of applications and is typically lower in cost than traditional SQL for similar volumes of data.
- Azure Table storage stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud. Azure tables are ideal for storing structured, non-relational data. Common uses of Table storage include:
- 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 can be denormalized for fast access
- You can use Table storage to store and query huge sets of structured, non-relational data, and your tables will scale as demand increases.

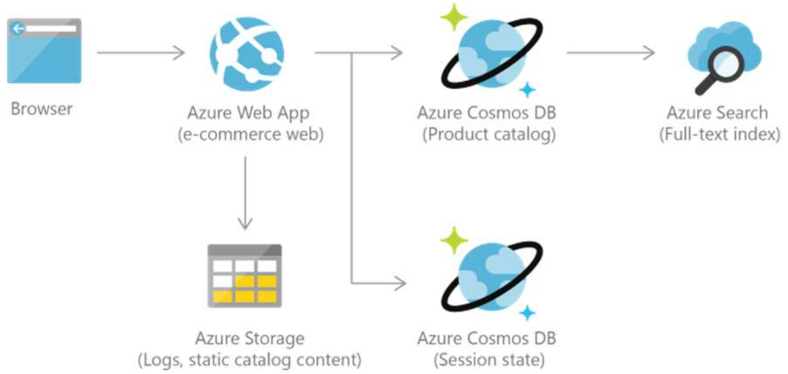
Overview of Azure Cosmos DB

- Azure Cosmos DB is a globally distributed and elastically scalable database. It has a guaranteed low latency that is backed by a comprehensive set of Service Level Agreements (SLAs). Consistency can sometimes be an issue when you are working with distributed systems, but Azure Cosmos DB alleviates this situation by offering you a sustained level of performance.

Retail and Marketing

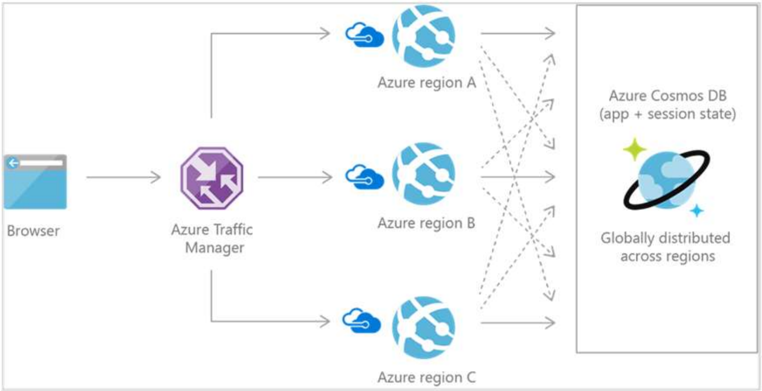
- Azure Cosmos DB is used extensively in Microsoft's own e-commerce platforms, that run the Windows Store and XBox Live. It is also used in the retail industry for storing catalog data and for event sourcing in order processing pipelines.
- Catalog data usage scenarios involve storing and querying a set of attributes for entities such as people, places, and products. Some examples of catalog data are user accounts, product catalogs, IoT device registries, and bill of materials systems. Attributes for this data may vary and can change over time to fit application requirements.

Consider an example of a product catalog for an automotive parts supplier. Every part may have its own attributes in addition to the common attributes that all parts share. Furthermore, attributes for a specific part can change the following year when a new model is released. Azure Cosmos DB supports flexible schemas and hierarchical data, and thus it is well suited for storing product catalog data.



Social Applications

- A common use case for Azure Cosmos DB is to store and query user generated content (UGC) for web, mobile, and social media applications. Some examples of UGC are chat sessions, tweets, blog posts, ratings, and comments. Often, the UGC in social media applications is a blend of free form text, properties and tags. Content such as chats, comments, and posts can be stored in Cosmos DB without requiring transformations or complex object to relational mapping layers. Data properties can be added or modified easily to match requirements as developers iterate over the application code, thus promoting rapid development.
- Applications that integrate with third-party social networks must respond to changing schemas from these networks. As data is automatically indexed by default in Cosmos DB, data is ready to be queried at any time. Hence, these applications have the flexibility to retrieve projections as per their respective needs.
- Many of the social applications run at global scale and can exhibit unpredictable usage patterns. Flexibility in scaling the data store is essential as the application layer scales to match usage demand.


Browser
Azure Traffic Manager
Azure region A
Azure region B
Azure region C
Azure Cosmos DB (app + session state)
Globally distributed across regions

Gaming

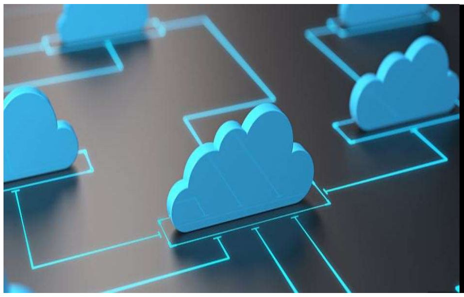
- The database tier is a crucial component of gaming applications. Modern games perform graphical processing on mobile/console clients, but rely on the cloud to deliver customized and personalized content like in-game stats, social media integration, and high-score leaderboards. Games often require single-millisecond latencies for reads and writes to provide an engaging in-game experience. A game database needs to be fast and be able to handle massive spikes in request rates during new game launches and feature updates.
- Azure Cosmos DB is used by games like **The Walking Dead: No Man's Land** by **Next Games**, and **Halo 5: Guardians**. Azure Cosmos DB provides the following benefits to game developers:

Gaming

- Azure Cosmos DB allows performance to be scaled up or down elastically. This allows games to handle updating profile and stats from dozens to millions of simultaneous gamers by making a single API call.
- Azure Cosmos DB supports millisecond reads and writes to help avoid any lags during game play.
- Azure Cosmos DB's automatic indexing allows for filtering against multiple different properties in real-time, for example, locate players by their internal player IDs, or their GameCenter, Facebook, Google IDs, or query based on player membership
- Social features including in-game chat messages, player guild memberships, challenges completed, high-score leaderboards, and social graphs are easier to implement with a flexible schema.
- Azure Cosmos DB as a managed platform-as-a-service (PaaS) required minimal setup and management work to allow for rapid iteration, and reduce time to market.

IoT and telematics

- IoT use cases commonly share some patterns in how they ingest, process, and store data. First, these systems need to ingest bursts of data from device sensors of various locales.
- Next, these systems process and analyze streaming data to derive real-time insights.
- The data is then archived to cold storage for batch analytics.
- Microsoft Azure offers rich services that can be applied for IoT use cases including Azure Cosmos DB, Azure Event Hubs, Azure Stream Analytics, Azure Notification Hub, Azure Machine Learning, Azure HDInsight, and Power BI.



Module 16:
Azure SQL

Topics Covered

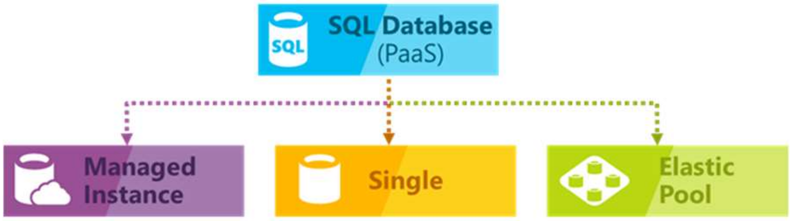
- ❑Understanding Azure SQL
- ❑Deployment Models
- ❑Business Continuity
- ❑High Availability

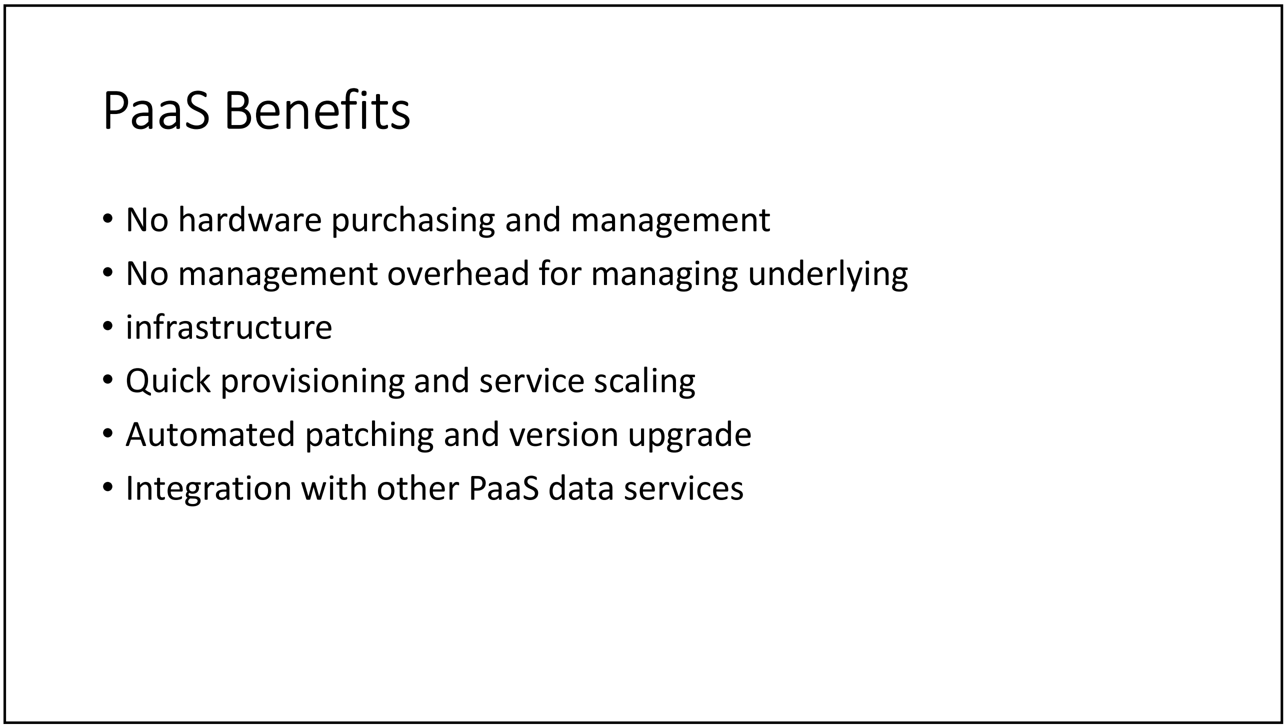
Implement Azure SQL Databases

- SQL Database is a fully managed Platform as a Service (PaaS) Database Engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement. Azure SQL Database is always running on the latest stable version of SQL Server Database Engine and patched OS with 99.99% availability.

Deployment models

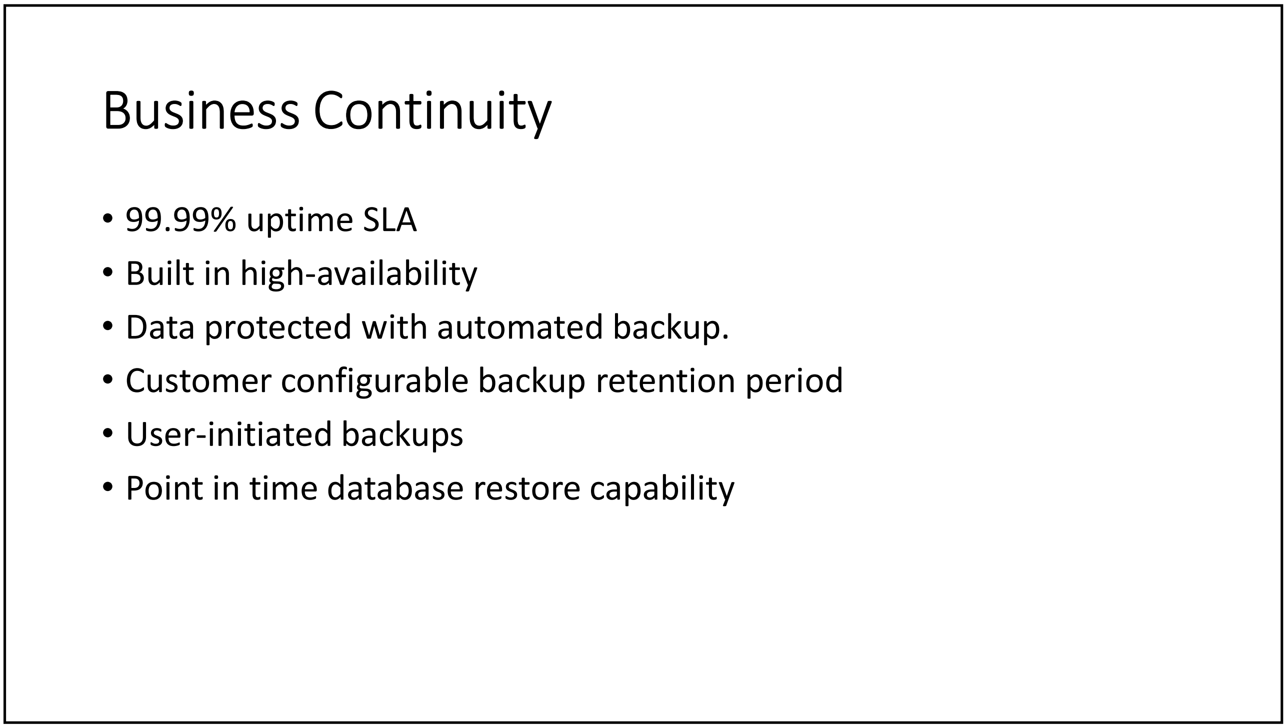
- **Single database** represents a fully managed, isolated database. You might use this option if you have modern cloud applications and microservices that need a single reliable data source.
- **Managed instance** is a fully managed instance of the Microsoft SQL Server Database Engine. It contains a set of databases that can be used together. Use this option for easy migration of on-premises SQL Server databases to the Azure cloud, and for applications that need to use the database features that SQL Server Database Engine provides.
- **Elastic pool** is a collection of single databases with a shared set of resources, such as CPU or memory. Single databases can be moved into and out of an elastic pool.





PaaS Benefits

- No hardware purchasing and management
- No management overhead for managing underlying
- infrastructure
- Quick provisioning and service scaling
- Automated patching and version upgrade
- Integration with other PaaS data services



Business Continuity

- 99.99% uptime SLA
- Built in high-availability
- Data protected with automated backup.
- Customer configurable backup retention period
- User-initiated backups
- Point in time database restore capability

High-Availability and Azure SQL Database

- There are two high-availability architectural models that are used in Azure SQL Database:
- **Standard availability model that is based on a separation of compute and storage**. It relies on high availability and reliability of the remote storage tier. This architecture targets budget-oriented business applications that can tolerate some performance degradation during maintenance activities.
- **Premium availability model that is based on a cluster of database engine processes**. It relies on the fact that there is always a quorum of available database engine nodes. This architecture targets mission critical applications with high IO performance, high transaction rate and guarantees minimal performance impact to your workload during maintenance activities.

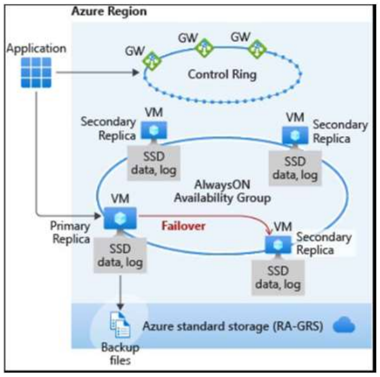
The standard availability model

The standard availability model includes two layers:

- A **stateless compute layer** that runs the sqlservr.exe process and contains only transient and cached data, such as TempDB, model databases on the attached SSD, and plan cache, buffer pool, and columnstore pool in memory. This stateless node is operated by Azure Service Fabric that initializes sqlservr.exe, controls health of the node, and performs failover to another node if necessary.
- A **stateful data layer** with the database files (.mdf/.ldf) that are stored in Azure Blob storage. Azure blob storage has built-in data availability and redundancy feature. It guarantees that every record in the log file or page in the data file will be preserved even if SQL Server process crashes.

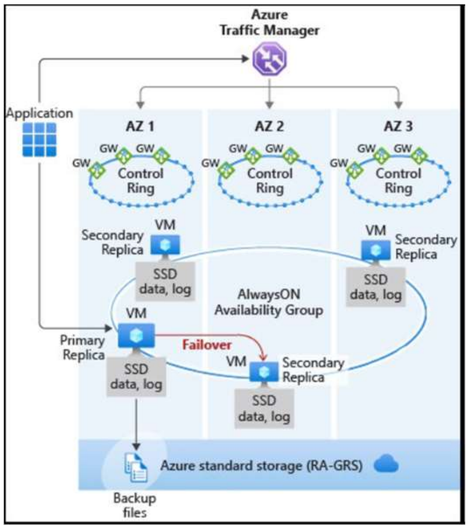
Premium and Business Critical service tier availability

Premium and Business Critical service tiers leverage the Premium availability model, which integrates compute resources (SQL Server Database Engine process) and storage (locally attached SSD) on a single node. High availability is achieved by replicating both compute and storage to additional nodes creating a three to four-node cluster.



Zone redundant configuration

- By default, the cluster of nodes for the premium availability model is created in the same datacenter. With the introduction of Azure Availability Zones, SQL Database can place different replicas of the Business Critical database to different availability zones in the same region. To eliminate a single point of failure, the control ring is also duplicated across multiple zones as three gateway rings (GW). The routing to a specific gateway ring is controlled by Azure Traffic Manager (ATM).



Social Media Content

https://RTSnetworking.com

- YouTube Channel
- Facebook Group