



Azure Champ

Azure Champ

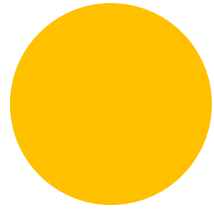




Onur Yüksektepeli | @oyuksektepeli

- Microsoft Cloud Solutions Architect
- Microsoft MVP, Microsoft MCT
- Community Lead
- V-onyuks@microsoft.com
- Onur.yuksektepeli@mshowto.org
- <https://twitter.com/oyuksektepeli>
- <https://www.linkedin.com/in/onuryuksektepeli/>
- <https://github.com/oyuksektepeli>
- <https://notebooks.azure.com/oyuksektepeli/>
- <http://www.youtube.com/c/onuryuksektepeli>
- <https://www.facebook.com/onuryuksektepeli/>





Azure Resource Groups

Azure Champ



Connect to Azure

Azure
Portal

Azure
Cloud Shell

Azure
Powershell

Azure CLI
v2.0

Azure
SDKs

Azure Cloud Shell

You have no storage mounted ✕

Azure Cloud Shell requires an Azure file share to persist files. [Learn more](#)
This will create a new storage account for you and this will incur a small monthly cost. [View pricing](#)

* Subscription

Diagnostics



[Show advanced settings](#)

Create storage

Close

Azure Cloud Shell

```
PowerShell | ? | ? | ? | ? | {}
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

MOTD: Scripts installed with 'Install-Script' can be run from the shell

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Azure:/
PS Azure:\> Get-CloudDrive

FileShareName      : cs-onur-yuksektepeli-yuksektek-com-1003bffd9f20c732
FileSharePath      : //csb7fd89b160998x418fxac1.file.core.windows.net/cs-onur-yuksektepeli-yuksektek-com-1003bffd9f20c732
MountPoint         : /home/onur/cloudrive
Name               : csb7fd89b160998x418fxac1
ResourceGroupName  : cloud-shell-storage-westeuropa
StorageAccountName : csb7fd89b160998x418fxac1
SubscriptionId     : 7fd89b16-0998-418f-ac17-236f38d101bc
```

```
Bash | ? | ? | ? | ? | {}
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

onur@Azure:~$ clouddrive -h

Group
  clouddrive                :Manage storage settings for Azure Cloud Shell.

Commands
  mount                     :Mount a file share to Cloud Shell.
  unmount                   :Unmount a file share from Cloud Shell.

onur@Azure:~$
```

Azure Cloud Drive

cloudshell

>_📁🔔⚙️?😊

Dashboard > Resource groups > cloud-shell-storage-west europe > csb7fd89b160998x418fxac1 - Files > cs-onur-yuksektepeli-yuksektek-com-1003bffd9f20c732

cs-onur-yuksektepeli-yuksektek-com-1003bffd9f20c732

File share

🔍 Search (Ctrl+/) <<

📄 Overview

👤 Access Control (IAM)

⚙️ Settings

🔑 Access policy

📁 Properties

🔗 Connect ⬆️ Upload ➕ Add directory ↻ Refresh 🗑️ Delete share ✎️ Quota 🔍 View snapshots 📸 Create Snapshot


📘 Backup (Preview) is not enabled for this file share. Click here to enable backup.

📍 Location: cs-onur-yuksektepeli-yuksektek-com-1003bffd9f20c732

🔍 Search files by prefix

NAME	TYPE	SIZE
📁 .cloudconsole	Directory	

Visual Studio


 | **Visual Studio** Visual Studio IDE Features ▾ Offerings ▾ Downloads Support ▾ Subscriber Access [Free Visual Studio](#)

All Microsoft ▾ Search 🔍 Sign in


Visual Studio Community

A fully-featured, extensible, free IDE for creating modern applications for Android, iOS, Windows, as well as web applications and cloud services.

[Windows](#) [macOS](#)


[Download Visual Studio](#) 

Everything you need all in one place




Flexibility

Build apps for any platform




Productivity

Designers, editors, debuggers, profilers, in one single tool



Ecosystem

Access to thousands of extensions

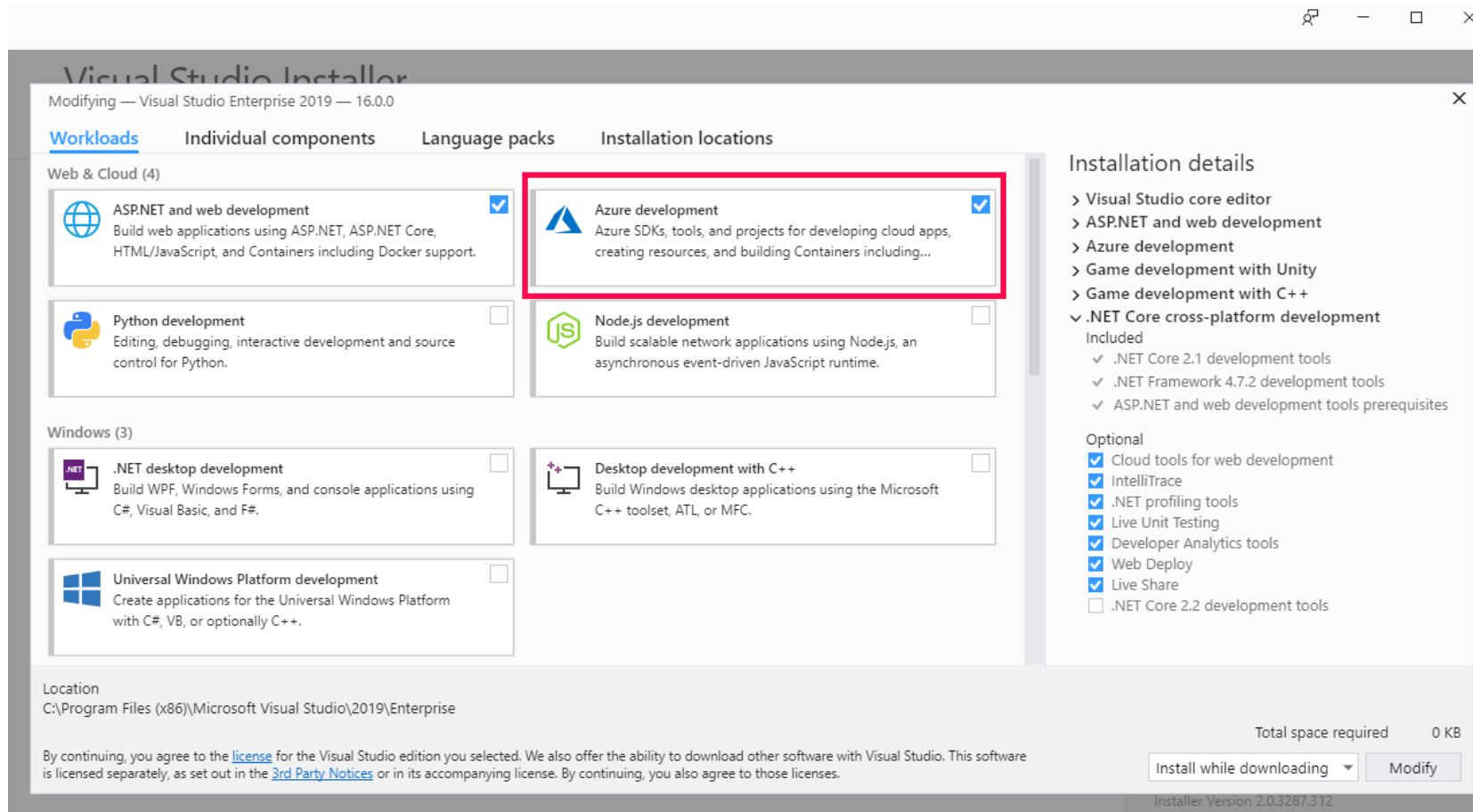


Languages

Code in C#, Visual Basic, F#, C++, HTML, JavaScript, TypeScript, Python, and more

<https://visualstudio.microsoft.com/vs/community/>

Azure Development



Azure Resource Groups

- Resources in a resource group should share the same lifecycle
- Each resource can only exist in one resource group
- Resources can be added or removed to a resource group at any time
- Resources can be moved from one resources group to another
- Resource groups can contain resources that reside in different regions
- Resources can interact with resources in other resources groups

Resource Group Management

- Tags
- Locks
- Access Control (IAM)
- Policies

Sample Resource Group

- Ms-net-rg
- Purpose: Isolate the Virtual networks
- Need: Prevent unwanted changes to any of the network resources
- Admin: It will deploy and maintain RG
- Notes: Resources in other RGs will use the resources int this group
- Dept: IT
- Owner: Onur YUKSEKTEPELI

Demo

- Creating a Resource

Azure Resource Tags

- Logically organize resources. Each tag has a name and a value. Allows related resources from different resource groups to be identified. Organize by billing and management.

TAG Rules

- Tags are NOT inherited
- Names can't contain these characters: <, >, %, &, \, ?, /
- Tag name is limited to 512 characters
- Tag value is limited to 256 characters

Demo

- Create Tag

Resource Group Locks

- Prevent accidental deletion or changes to resources in resource groups. Consists of two locks:
 - CanNotDelete
 - ReadOnly

Demo

- Create Resource Locks

Access Control (IAM)

- A system that provides fine-grained access Management of resources in Azure. Grant only the amount of Access to users needed to perform their jobs

Demo

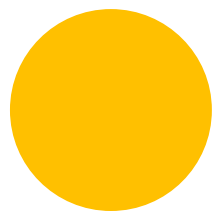
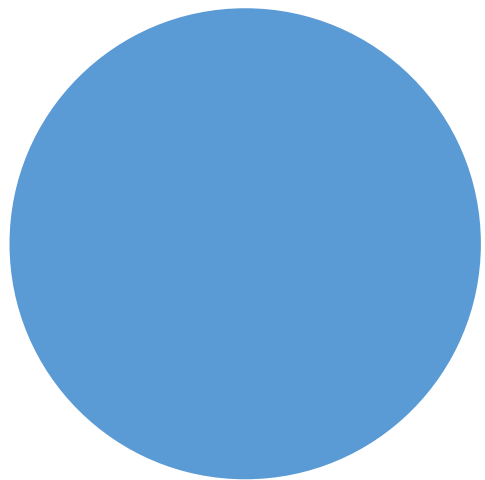
- Access Control (IAM)

Azure Policy

- Allows you to manage and prevent IT issues with policy definitions that enforce rules and effects for your resources. Policies allow you to keep compliant with corporate standards and SLAs.

Demo

- Azure Policy



Azure Compute

Azure Champ



Azure Compute

- Azure Compute Unit

The concept of the Azure Compute Unit (ACU) provides a way of comparing compute (CPU) performance across Azure SKUs. This will help you easily identify which SKU is most likely to satisfy your performance needs. ACU is currently standardized on a Small (Standard_A1) VM being 100 and all other SKUs then represent approximately how much faster that SKU can run a standard benchmark.

Azure Compute Unit(ACU)

SKU Family	ACU \ vCPU	vCPU: Core
A0	50	1:1
A1 - A4	100	1:1
A5 - A7	100	1:1
A1_v2 - A8_v2	100	1:1
A2m_v2 - A8m_v2	100	1:1
A8 - A11	225*	1:1
D1 - D14	160 - 250	1:1
D1_v2 - D15_v2	210 - 250*	1:1
DS1 - DS14	160 - 250	1:1
DS1_v2 - DS15_v2	210 - 250*	1:1
D_v3	160 - 190*	2:1***
Ds_v3	160 - 190*	2:1***
E_v3	160 - 190*	2:1***
Es_v3	160 - 190*	2:1***
F2s_v2 - F72s_v2	195 - 210*	2:1***
F1 - F16	210 - 250*	1:1
F1s - F16s	210 - 250*	1:1
G1 - G5	180 - 240*	1:1
GS1 - GS5	180 - 240*	1:1
H	290 - 300*	1:1

Azure Virtual Machines

	General Purpose	Compute Optimized	Memory Optimized	Storage Optimized	GPU	High Performance Compute
Type	DC, Av2, Dv2, Dv3, B, Dsv3	Fsv2, F	M, Dv2, G, Dsv2, GS, Ev3	Ls	NC, NCv2, ND, BV, NVv2	H
Description	Balanced CPU and memory	High ratio of compute to memory	High ratio of memory to compute	High disk throughput and IO	Specialized with single or multiple NVIDIA GPUs	High memory and compute power – fastest and most powerful
Uses	Testing and dev, small-med databases, low traffic web servers	Medium traffic web servers, network appliances, batch processing, app servers	Relational database services, analytics, and larger caches	Big Data, SQL, NoSQL databases	Compute intensive, graphics-intensive, and visualization workloads	Batch processing, analytics, molecular modeling, and fluid dynamics, low latency RDMA networking

Standard vs. Premium Storage Disks

Standard Disks	Premium Disks
Backed by cost-effective HDDs	Backed by high-speed SSDs
Stored in Azure storage account	IOPS values are predictable, expected performance levels
Standard SSD (Preview) available for managed disks (dev/test/entry level production applications)	Pre-pay for all storage used (fixed disk sizes P10, 128 GB, 500 IOPs, 50 MB/sec
Standard storage provides maximum IOPS values for each VHD	

Managed vs. Unmanaged Disks

Unmanaged Disks	Managed Disks
Original method to store VM VHDs	Azure manages the disks, so you don't have to worry about storage account level IOPS restrictions
VHDs stored as page blobs in an Azure storage account	Pre-pay for disk size (no need for SA) S10, 128 GB, 500 IOPS, 60 MB/sec
Maximum 256 TB of storage per VM	Supports Standard and Premium SSD and Standard HDD
You need to manage storage account availability	
20,000 IOPS limit across all VM disks in a standard storage account	

Ultra SSD – the next generation of Azure Disks technology

Ultra SSD

supported VM types will be limited

Ultra SSD Disks come in several fixed sizes from 4 GiB up to 64 TiB and feature a flexible performance configuration model that allows you to independently configure IOPS and throughput.

Ultra SSDs support IOPS limits of 300 IOPS/GiB, up to a maximum of 160K IOPS per disk. To achieve the IOPS that you provisioned, ensure that the selected Disk IOPS is less than the VM IOPS.

With Ultra SSD Disks, the throughput limit of a single disk is 256 KiB/s for each provisioned IOPS, up to a maximum of 2000 MBps per disk (where MBps = 10^6 Bytes per second).

Azure Ultra SSD

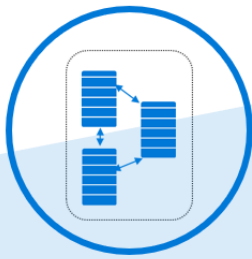
Ultra SSD Managed Disk Offerings

Disk size (GiB)	4	8	16	32	64	128	256	512	1,024-65,536 (in increments of 1 TiB)
IOPS range	100-1,200	100-2,400	100-4,800	100-9,600	100-19,200	100-38,400	100-76,800	100-153,600	100-160,000
Throughput Cap (MBps)	300	600	1,200	2,000	2,000	2,000	2,000	2,000	2,000

Planning High Availability



Availability Sets



Availability Zones



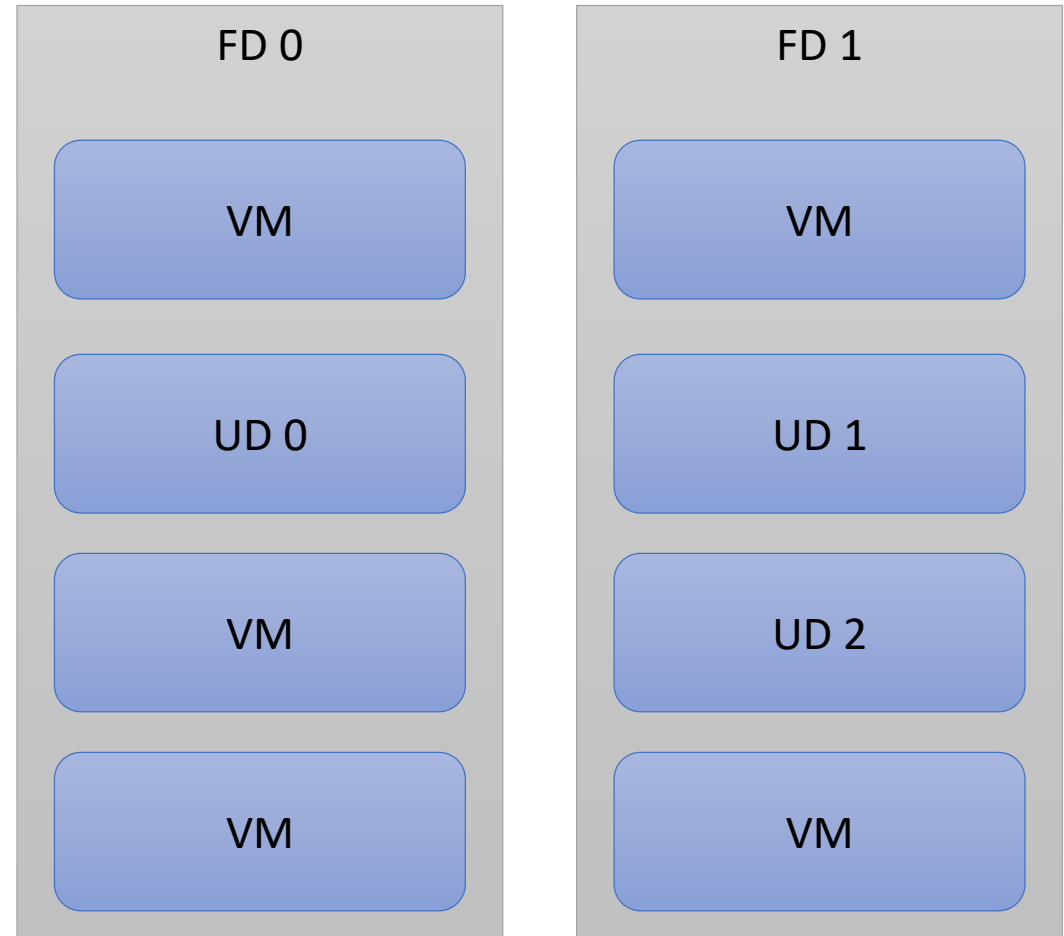
Region Pairs

Blast Radius

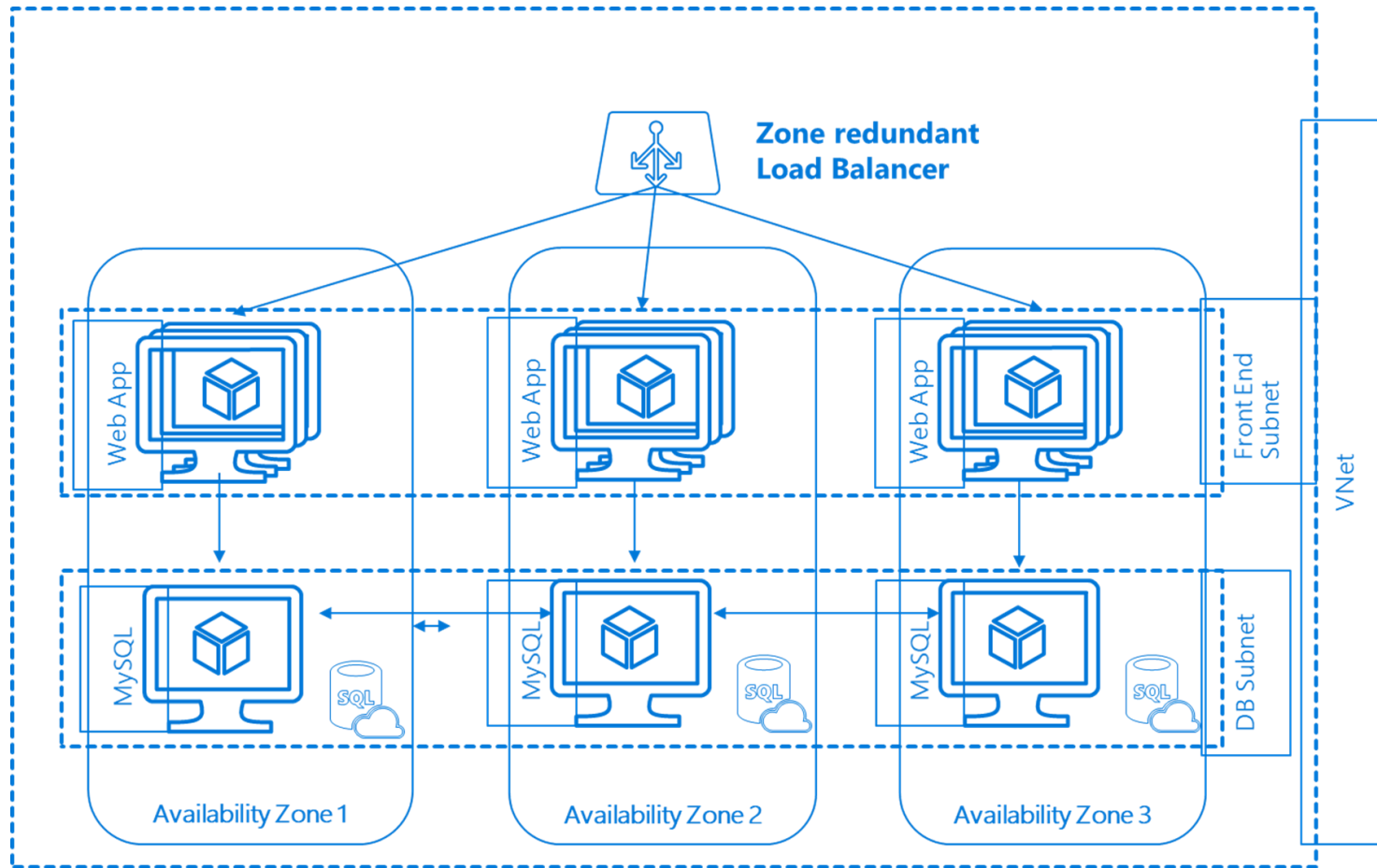
Feature	Capability / Provide
Availability Sets	High-availability protection from hardware, network, and power failures in a DC
Availability Zones	High-availability protection against the loss of entire DC(s)
Region pairs	Disaster Recovery that protects from the loss of an entire region

Availability Sets

- %99.95 Availability SLA with Availability set
- Must be configured at VM Deployment
- Otherwise %99.9 single instance SLA with Premium storage

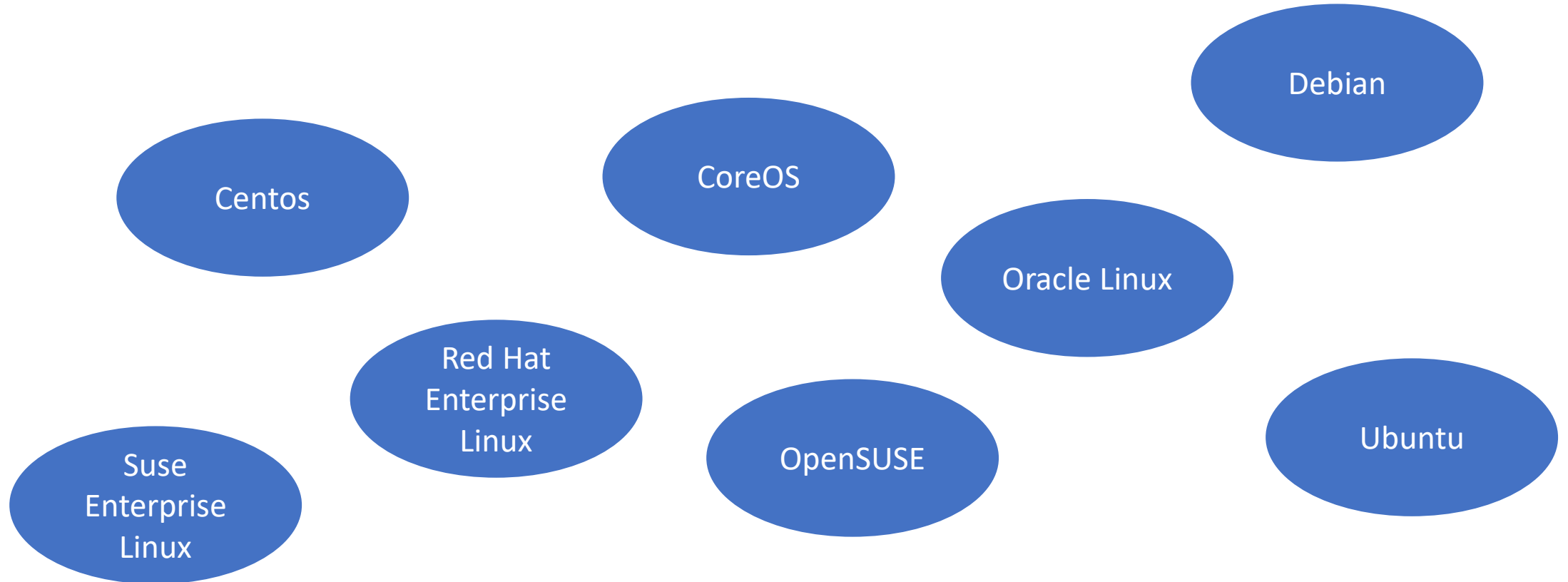


Availability Zone



<http://aka.ms/azoverview>

Supported Linux Distributions in Azure



<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros>

Azure Deployment Tools

Azure Portal

Azure Cloud Shell

Azure Powershell

Azure CLI v2.0

Azure SDKs

ARM Templates



Demo

- Deploy a Linux VM in Azure
- Deploy a Windows VM in Azure with Visual Studio



Demo

Connect Windows VM via Serial

Azure VM Disk Types

OS Disk	Data Disk	Temporary Disk
Generation 1 .VHD	# dependent on VM instance size	D: or /dev/sdb1
Registered as SATA drive	Registered as SCSI disk	Bound to the hardware host
Max capacity 2 TB	Max capacity 4 TB	Do not store permanent data!

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disks-types>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-types>

Demo

- Add Data Disk to VM

Demo

- Deploy VM from Existing Managed Disk

Demo

- Extend the Managed Disk

Demo

- Convert to Managed Disk

Demo

- Azure Disk Encryption

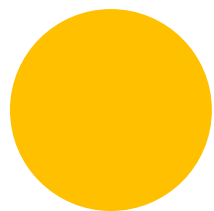
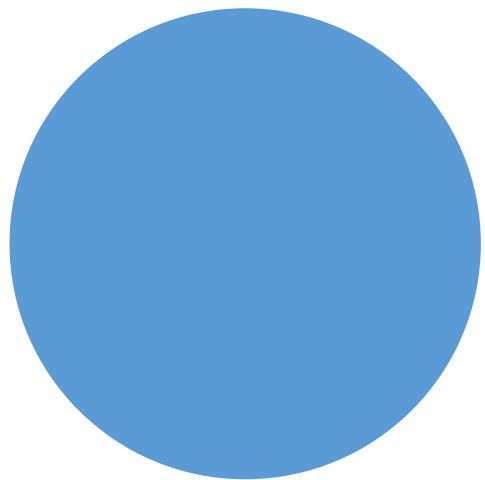
Move Azure Resources

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-move-resources>



Demo

Move Azure Resources



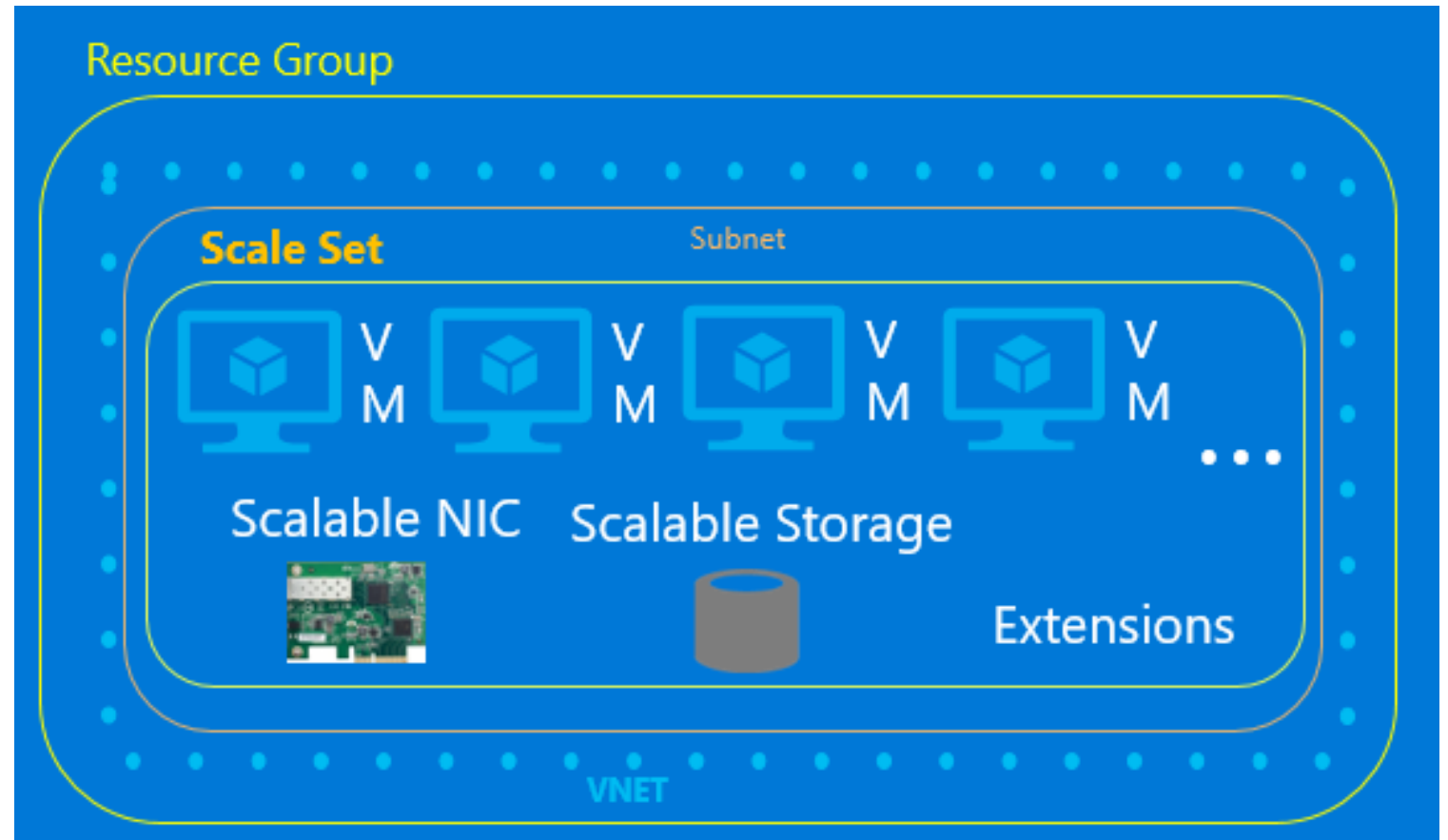
Virtual Machine Scale Set

Azure Champ



Azure Virtual Machine Scale Set

- Control it like IaaS, scale it like PaaS





Demo

Azure Virtual Machine Scale Test



Microsoft Identity

Azure Champ

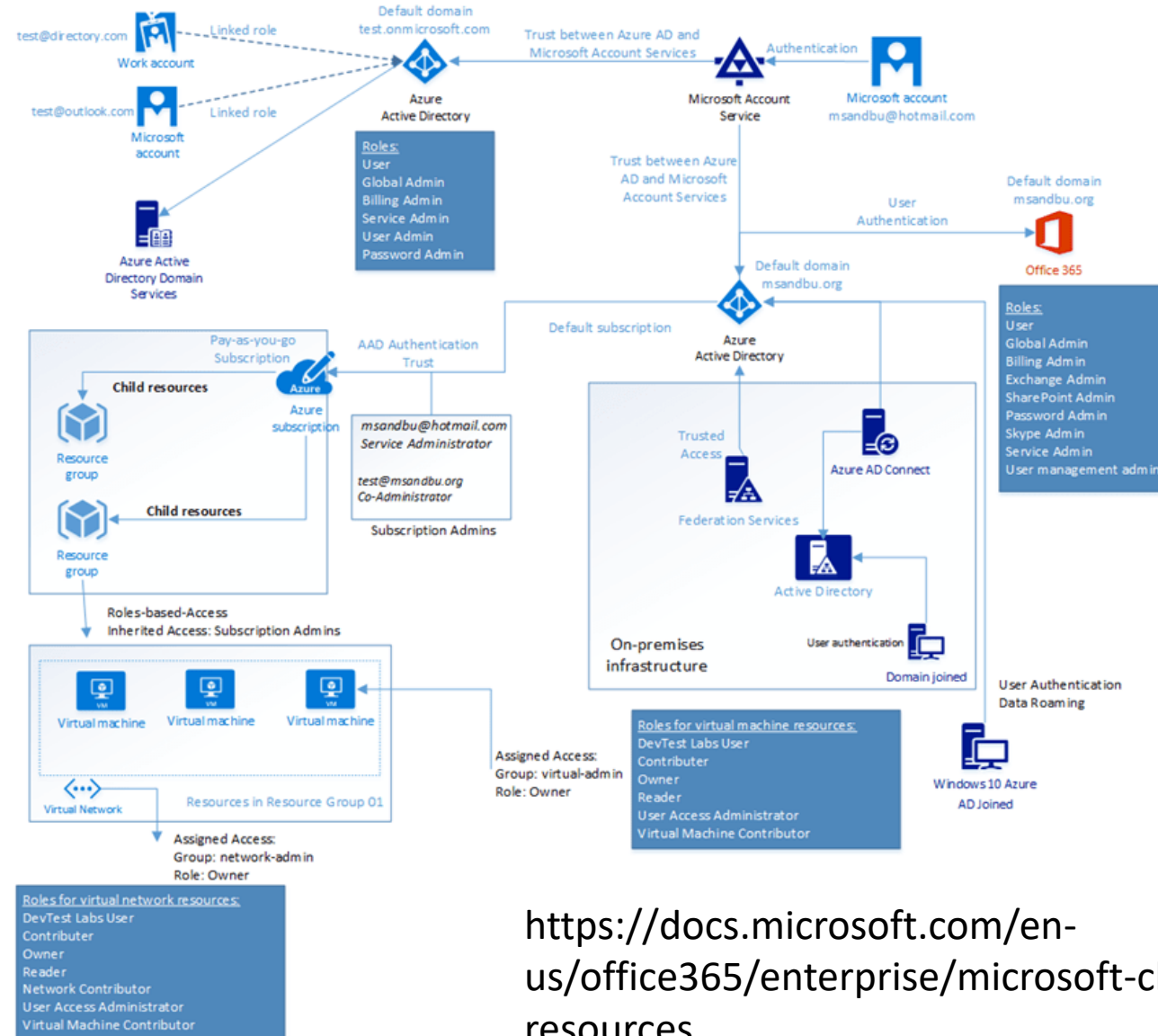


Terminology

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>

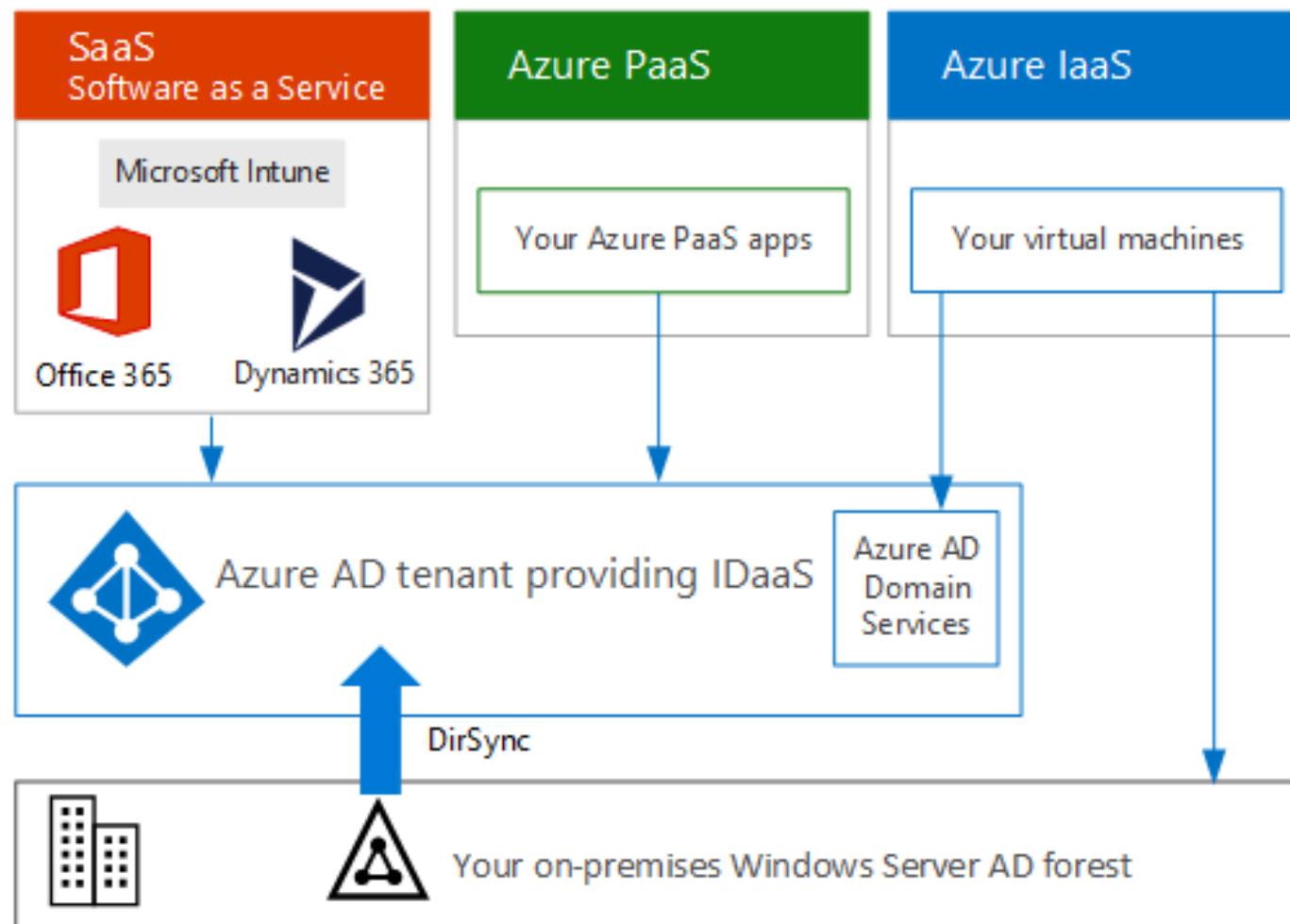
Azure subscription	Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
Azure tenant	A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription, such as Microsoft Azure, Microsoft Intune, or Office 365. An Azure tenant represents a single organization.
Azure AD directory	Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.
Custom domain	Every new Azure AD directory comes with an initial domain name, domainname.onmicrosoft.com. In addition to that initial name, you can also add your organization's domain names, which include the names you use to do business and your users use to access your organization's resources, to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as alain@contoso.com.

Microsoft Identity



<https://docs.microsoft.com/en-us/office365/enterprise/microsoft-cloud-it-architecture-resources>

Cloud-based Identity as a Service (IDaaS)



1 Security principal



User



Group



Service
principal



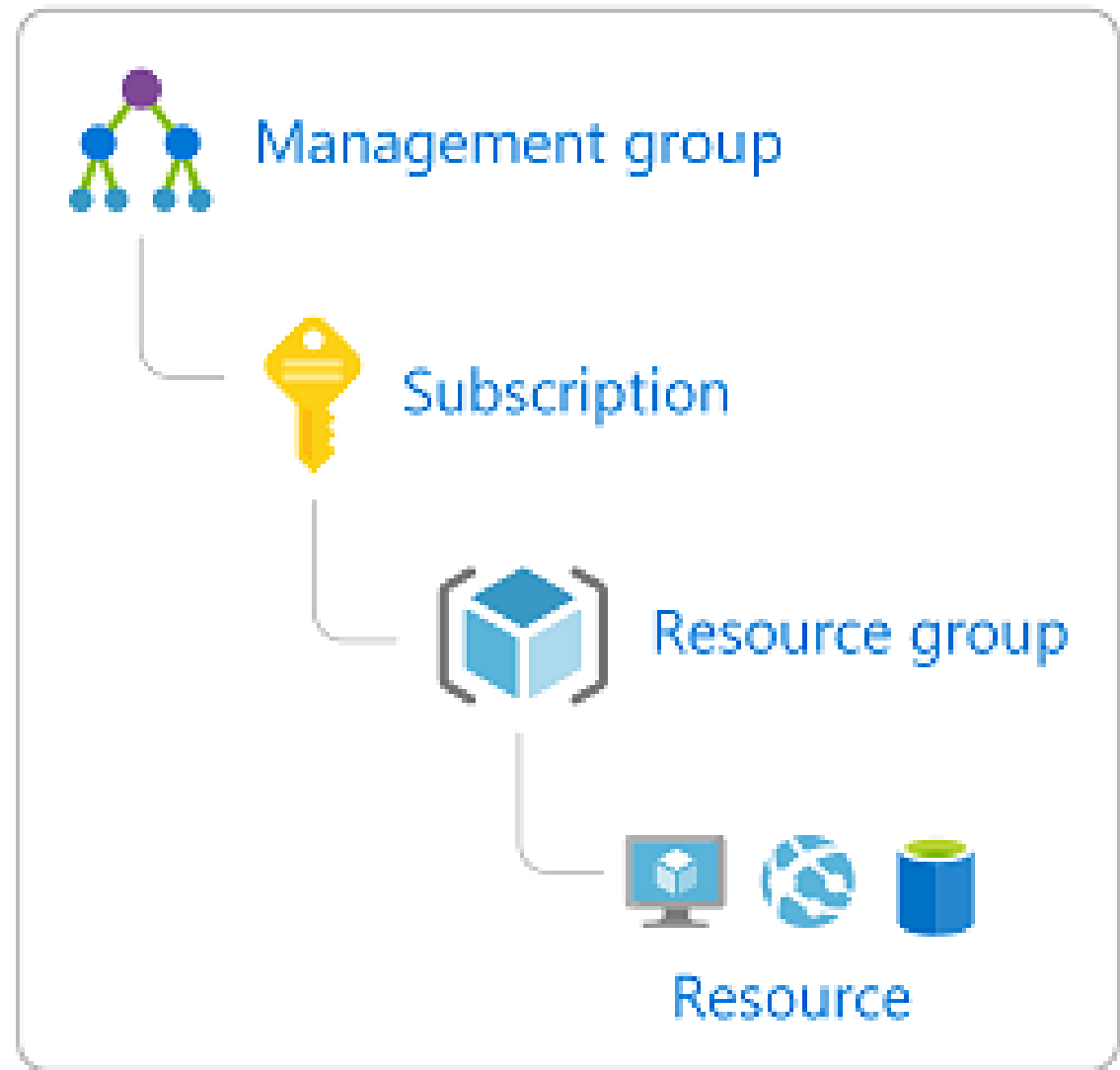
Managed
identity

- A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources.




Security Principal

Scope

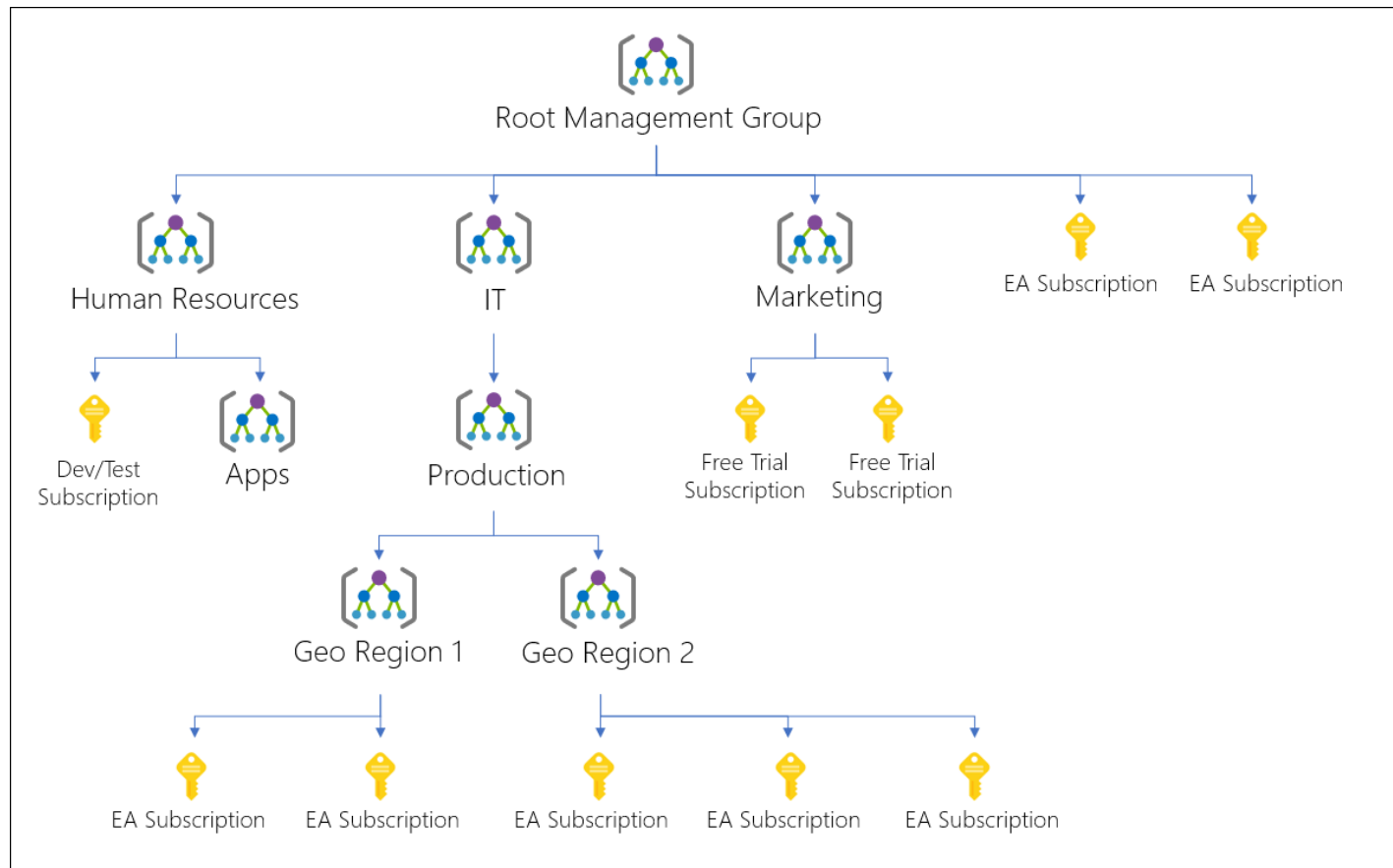
3 Scope



(RBAC) for Azure resources

		Role			
		Reader	Resource-specific or custom role	Contributor	Owner
Scope	 Subscription	Observers	Users managing resources		Admins
	 Resource group				
	 Resource	Automated processes			

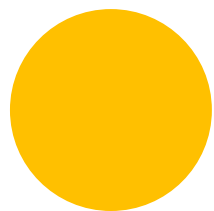
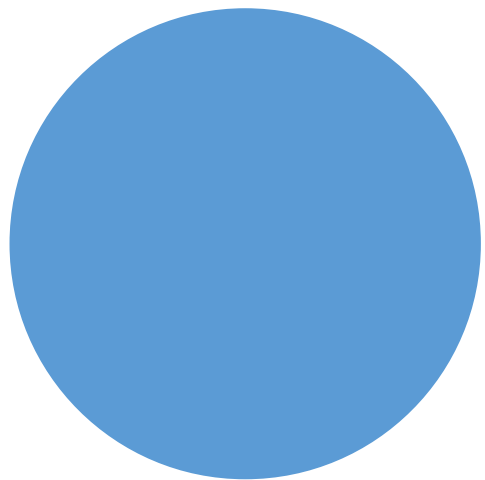
Management Groups





Demo

IAM in Resources



Azure Blob Storage

Azure Champ



Azure Storage Accounts

- Storage Account is parent container for storage types.

Blob Storage
Object and Disk
Storage

File Storage
SMB File Shares

Table Storage
NoSQL Data Store

**Queue
Storage**
Message Based

Azure Storage Account Links

- [http://mystorageaccount.**blob**.core.windows.net](http://mystorageaccount.blob.core.windows.net)
- [http://mystorageaccount.**file**.core.windows.net](http://mystorageaccount.file.core.windows.net)
- [http://mystorageaccount.**table**.core.windows.net](http://mystorageaccount.table.core.windows.net)
- [http://mystorageaccount.**queue**.core.windows.net](http://mystorageaccount.queue.core.windows.net)

Storage HA Levels

- Locally redundant storage (LRS): Low-cost data redundancy for Azure Storage

Locally redundant storage (LRS) provides at least 99.999999999% (11 nines) durability of objects over a given year. LRS provides this object durability by replicating your data to a storage scale unit.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-lrs?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

Storage HA Levels

- Zone-redundant storage (ZRS): Highly available Azure Storage applications

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region. Each storage cluster is physically separated from the others and is located in its own availability zone (AZ).

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

Storage HA Levels

- Geo-redundant storage (GRS): Cross-regional replication for Azure Storage

Geo-redundant storage (GRS) is designed to provide at least 99.999999999999999% (16 9's) durability of objects over a given year by replicating your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

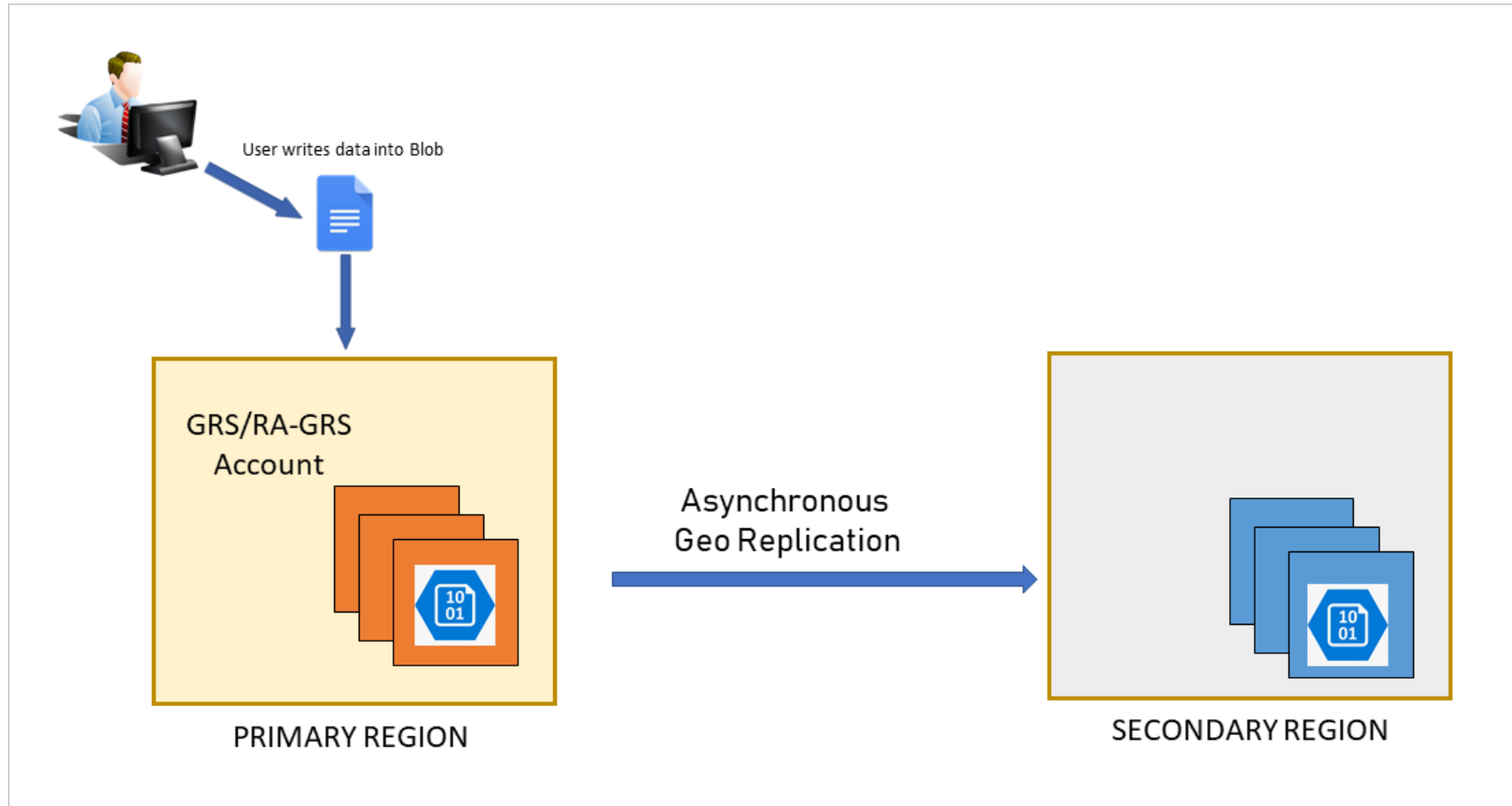
<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

Storage HA Levels

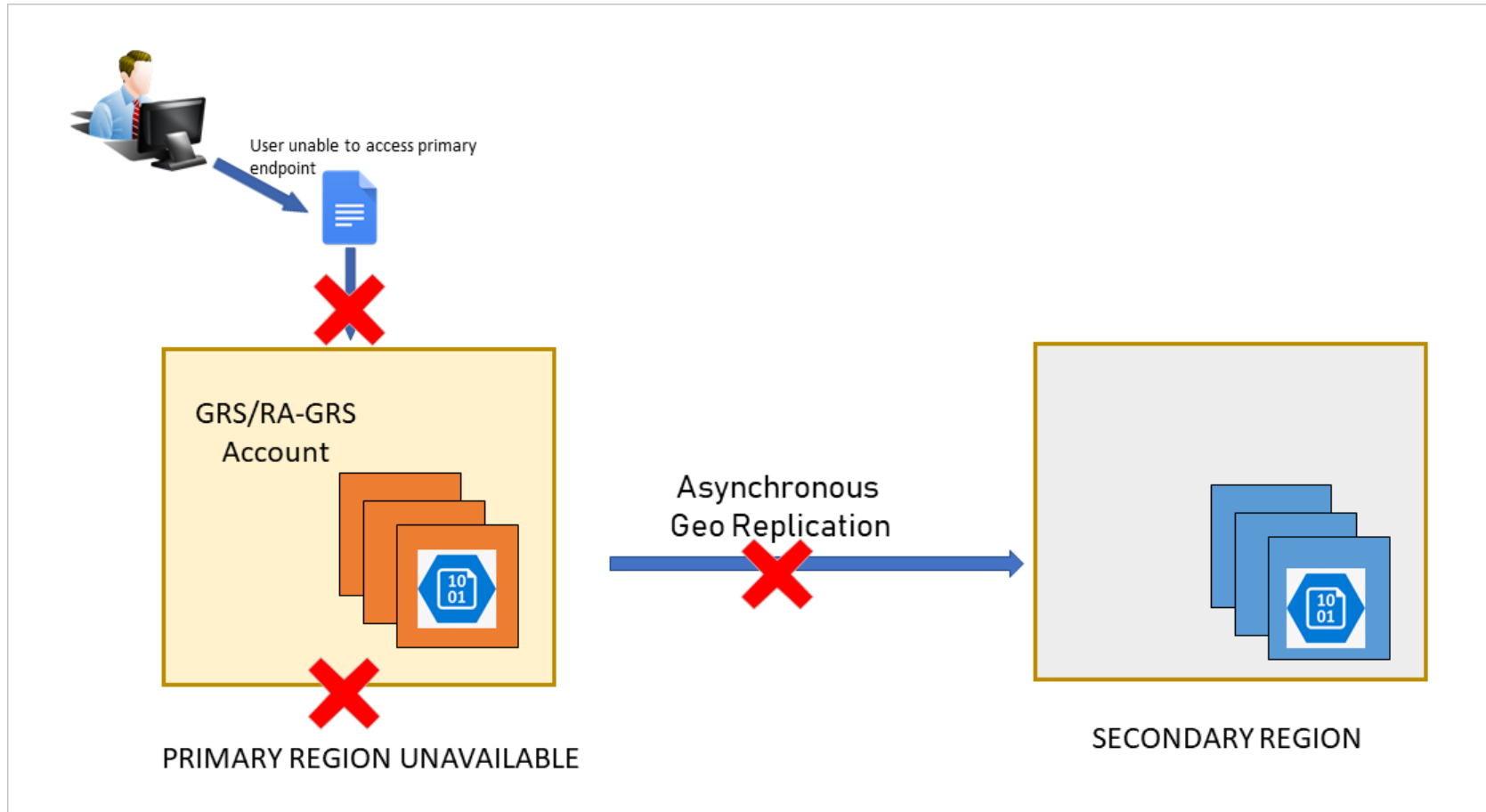
- Read-access geo-redundant storage (RA-GRS) is based on GRS. RA-GRS replicates your data to another data center in a secondary region, and also provides you with the option to read from the secondary region.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

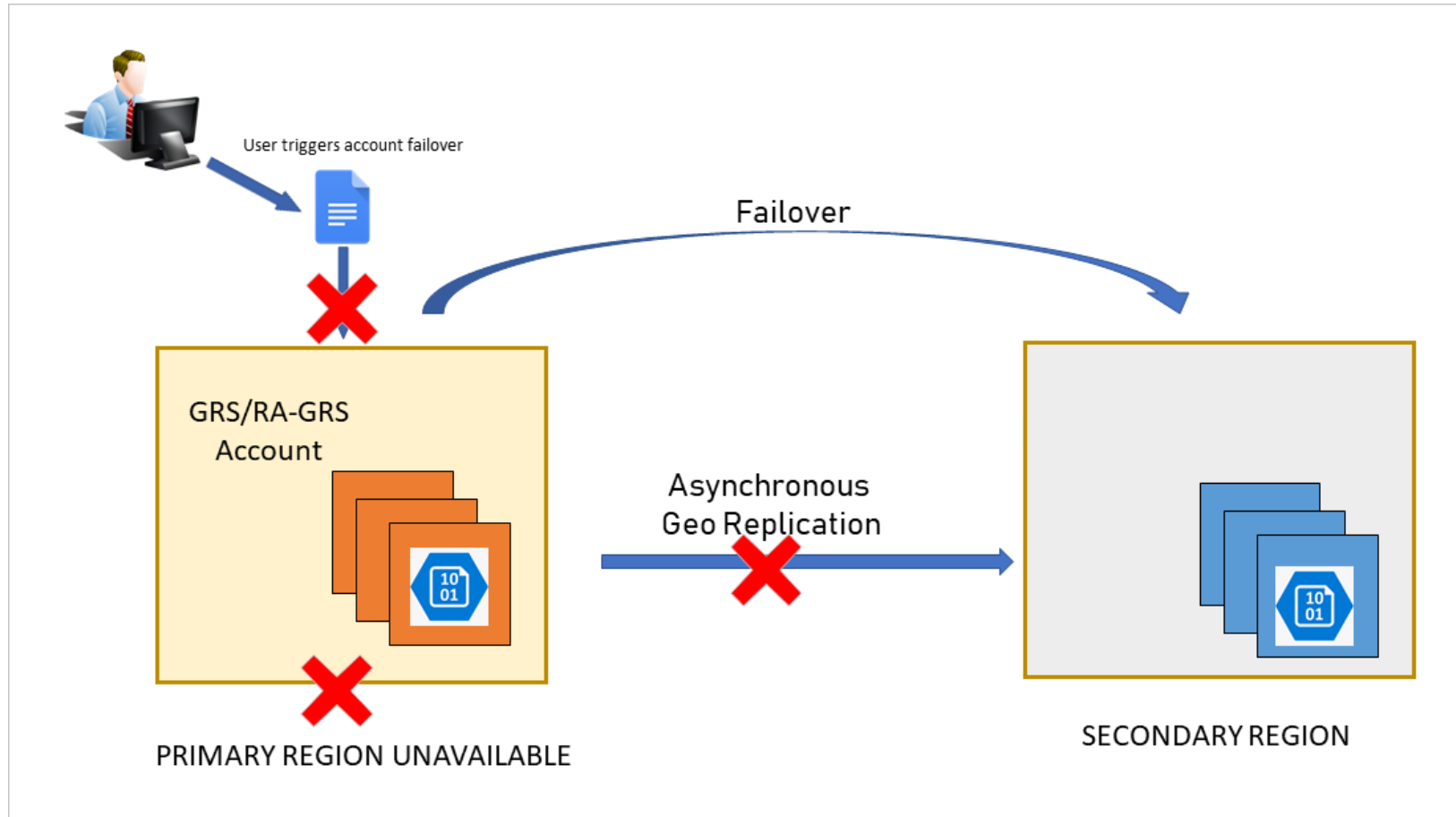
Storage HA Process



Storage HA Process



Storage HA Process



What is the RPO and RTO with GRS?

- The RPO indicates the point in time to which data can be recovered. Azure Storage typically has an RPO of less than 15 minutes, although there's currently no SLA on how long geo-replication takes.
- **Recovery Time Objective (RTO):** The RTO is a measure of how long it takes to perform the failover and get the storage account back online. The time to perform the failover includes the following actions:
 - The time until the customer initiates the failover of the storage account from the primary to the secondary region.
 - The time required by Azure to perform the failover by changing the primary DNS entries to point to the secondary location.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

Azure Storage Account Types



General Purpose v1

Blob

General Purpose v2

Azure Storage Account Limits

- <https://docs.microsoft.com/en-us/azure/storage/common/storage-scalability-targets>

Contact Azure Support if you need more!

Azure Storage Blob Service

- BLOB (Binary Large Object)
 - File, document, image, video, VM Disk, database etc.

<https://docs.microsoft.com/en-us/rest/api/storageservices/understanding-block-blobs--append-blobs--and-page-blobs>

Blob Types



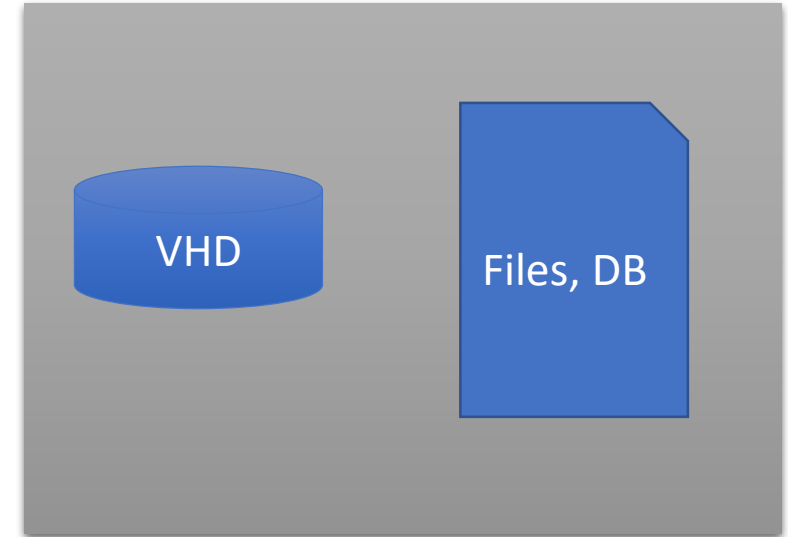
Block Blob

- Block blobs are comprised of blocks
- Each of which is identified by a block ID
- Each block can be a different size, up to a maximum of 100 MB
- Block blob can include up to 50,000 blocks
- Insert, replace, delete blocks supported
- MAX 4.77 TB



Append Blob

- is optimized for append operations
- blocks are added to the end of the blob only
- Updating or deleting of existing blocks is not supported
- append blob does not expose its block IDs.
- Each block in an append blob can be a different size, up to a maximum of 4 MB
- Ideal for logging, auditing
- MAX 195 GB



Page Blob

- collection of 512-byte pages optimized for random read and write operations
- Azure virtual machine disks are backed by page blobs
- Azure offers two types of durable disk storage: premium and standard
- MAX 8TB

Azure Storage Pricing

Data Storage (Capacity)

Data Operations

Output Data Transfer

Geo-Replication Data Transfer

Blob Storage Tiers

Hot Storage Tier

Highest Storage Cost
Lowest Data Access Cost

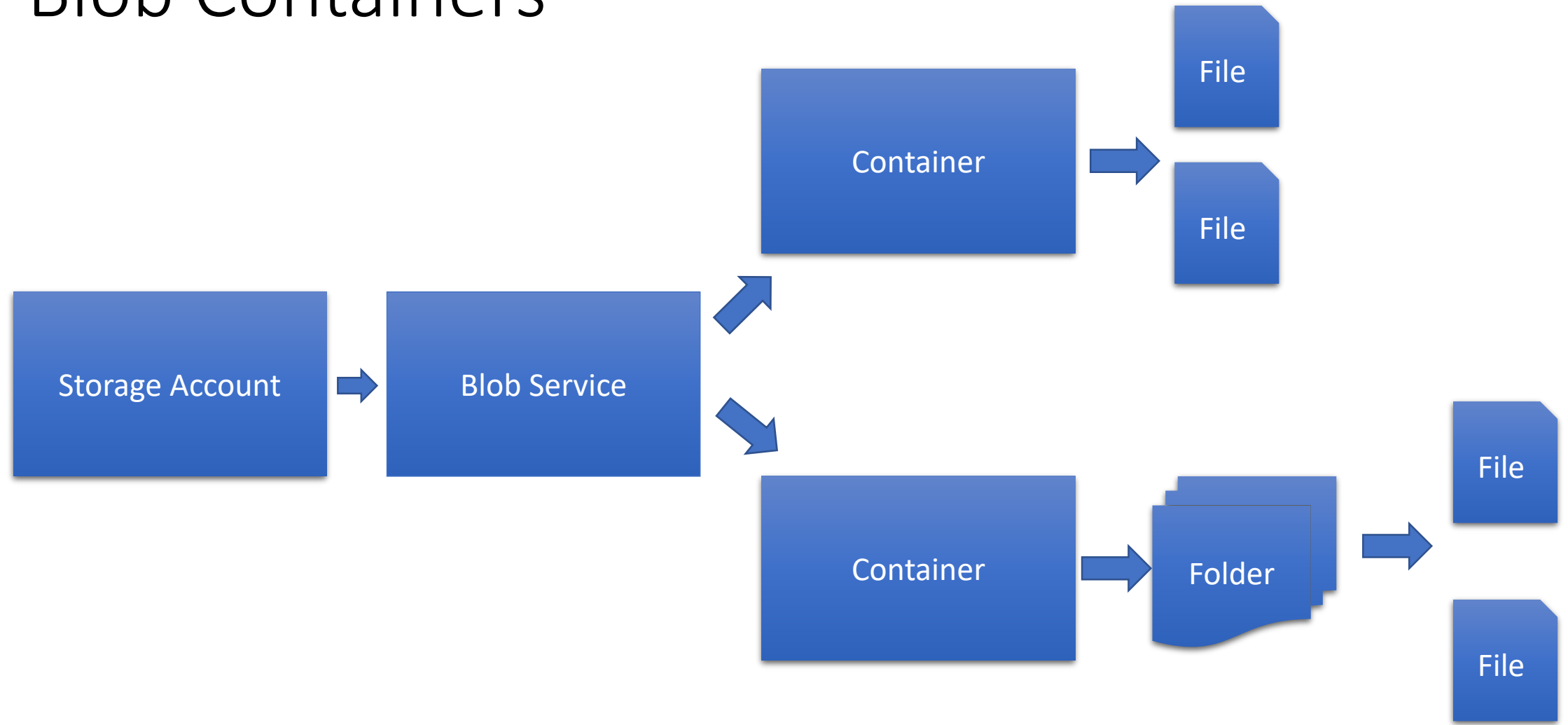
Cool Storage Tier

Higher Data Access Cost
Lower storage cost

Archive Storage Tier

Lowest storage cost
Highest data retrieval cost
Data is offline

Blob Containers



Public Access Level Container

- Private Access Level (by default)
Requires Authentication
- Public read access for blobs only: Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container.
- Full public read access: All container and blob data can be read by anonymous request. Clients can enumerate blobs within the container by anonymous request, but cannot enumerate containers within the storage account.

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-manage-access-to-resources>



Demo

Create a Storage Account from portal

Demo

Create a Storage Account from command line



Demo

Blob properties and create blob snapshot

Write Once Read Many (WORM)

- To prevent modification or deletion of data
- Configured at Blob Storage Container Level
- Time based retention period
- Legal hold retention
- No Additional cost to enable WORM



Demo

Enable WORM

Manage the Azure Blob storage Lifecycle

```
{
  "rules": [
    {
      "name": "ruleFoo",
      "enabled": true,
      "type": "Lifecycle",
      "definition": {
        "filters": {
          "blobTypes": [ "blockBlob" ],
          "prefixMatch": [ "container1/foo" ]
        },
        "actions": {
          "baseBlob": {
            "tierToCool": { "daysAfterModificationGreaterThan": 30 },
            "tierToArchive": { "daysAfterModificationGreaterThan": 90 },
            "delete": { "daysAfterModificationGreaterThan": 2555 }
          },
          "snapshot": {
            "delete": { "daysAfterCreationGreaterThan": 90 }
          }
        }
      }
    }
  ]
}
```

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts>



Demo

Blob Storage Lifecycle Management

Soft Delete

- Enable you to save and recover your blob data in many cases where blob are deleted.



Demo

Enable Soft Delete



Demo

Static Web Sites in Storage Account

Azure Storage Connection Options

- Azure Storage Explorer
- AzCopy Command line Utility
- Azure CLI
- Client Libraries (.net,java,python,php,node.js etc.)

Authentication Options for Azure Blob Storage

- Storage Account Key
- Shared Access Signature
- RBAC with Azure Active Directory

Shared Access Signature

- String containing a security token
- Can be appended to end of URL
- Access can be scoped to Container or Blob
- Specify permissions (read, write, delete, list)
- Validity Period start and end

Stored Access Policy

- Group of permissions
- Shared Access Signature can reference policy
- Revoking Stored Access Policy also revokes all referencing SAS tokens

Azure Active Directory RBAC

- Available for blob and Queue Services
- Users, Groups, Applications, Managed Service Identities
- Azure AD provide OAuth 2.0 Token
- Scope: Subscription, Resource Group, Storage Account, Blob Container
- Built-In role:
 - Storage Blob Data Contributor
 - Storage Blob Data Reader
- Https Only



Demo

Azure Storage Explorer

AzCopy

- No limit to number of files in batch
- Pattern filters to select files
- Can continue batch after connection interruption
- Only copy newer/older files
- Modify file name and metadata during upload
- Throttle number of concurrent connections
- Generate log file
- SAS or Storage Account



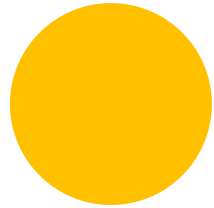
Demo

AzCopy



Demo

Az CLI



Azure CDN

Azure Champ



The background of the slide features a series of concentric, curved lines in a light gray color, creating a sense of motion or a globe-like effect. These lines are more prominent on the left side and fade out towards the right.

Azure CDN

- Distributed network of Servers
- Provide data to users from closest source
- Offload traffic from origin servers to CND
- Typically static data

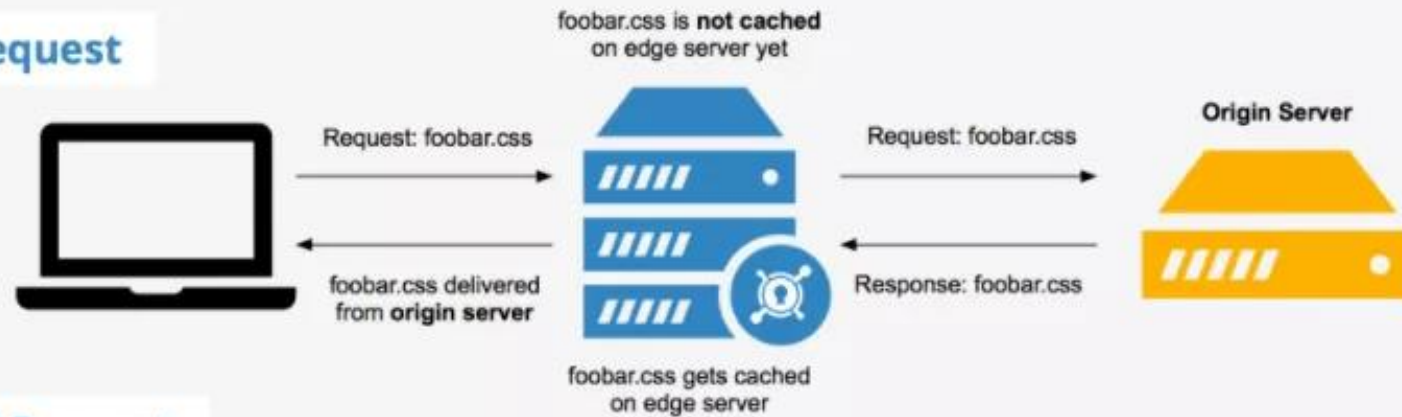
Azure CDN

- Azure Storage blob service are 'origin server'
- Azure CDN servers are 'edge servers'

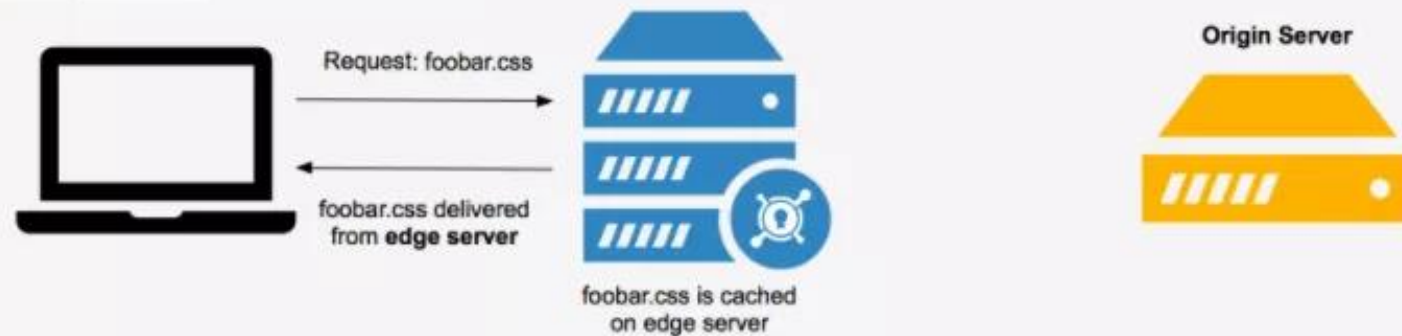
<https://docs.microsoft.com/en-us/azure/cdn/cdn-features>

Azure CDN

First Request



Second Request



Azure CDN Features

- HTTPS with Azure CDN Managed certificate
- Apply file compression to certain file types
- Large file download optimization
- Geo-filtering to restrict content by country

Azure CDN Features

Azure CDN Core Analytics

- Export to:
 - Blob Storage
 - Event Hubs
 - Log Analytics
- Metrics collected:
 - Number of request served from cache
 - Number of request retrieved from origin servers
 - GB of outbound data
 - HTTP status code returned to callers
 - Additional logging in Verizon Premium



Demo

Enabling Azure CDN

Azure CDN Caching Behaviour

- Bypass cache: Do not cache and ignore origin-provided cache-directive headers.
- Override: Ignore origin-provided cache duration; use the provided cache duration instead. This will not override cache-control: no-cache.
- Set if missing: Honor origin-provided cache-directive headers, if they exist; otherwise, use the provided cache duration.

Azure CDN caching behavior with query strings

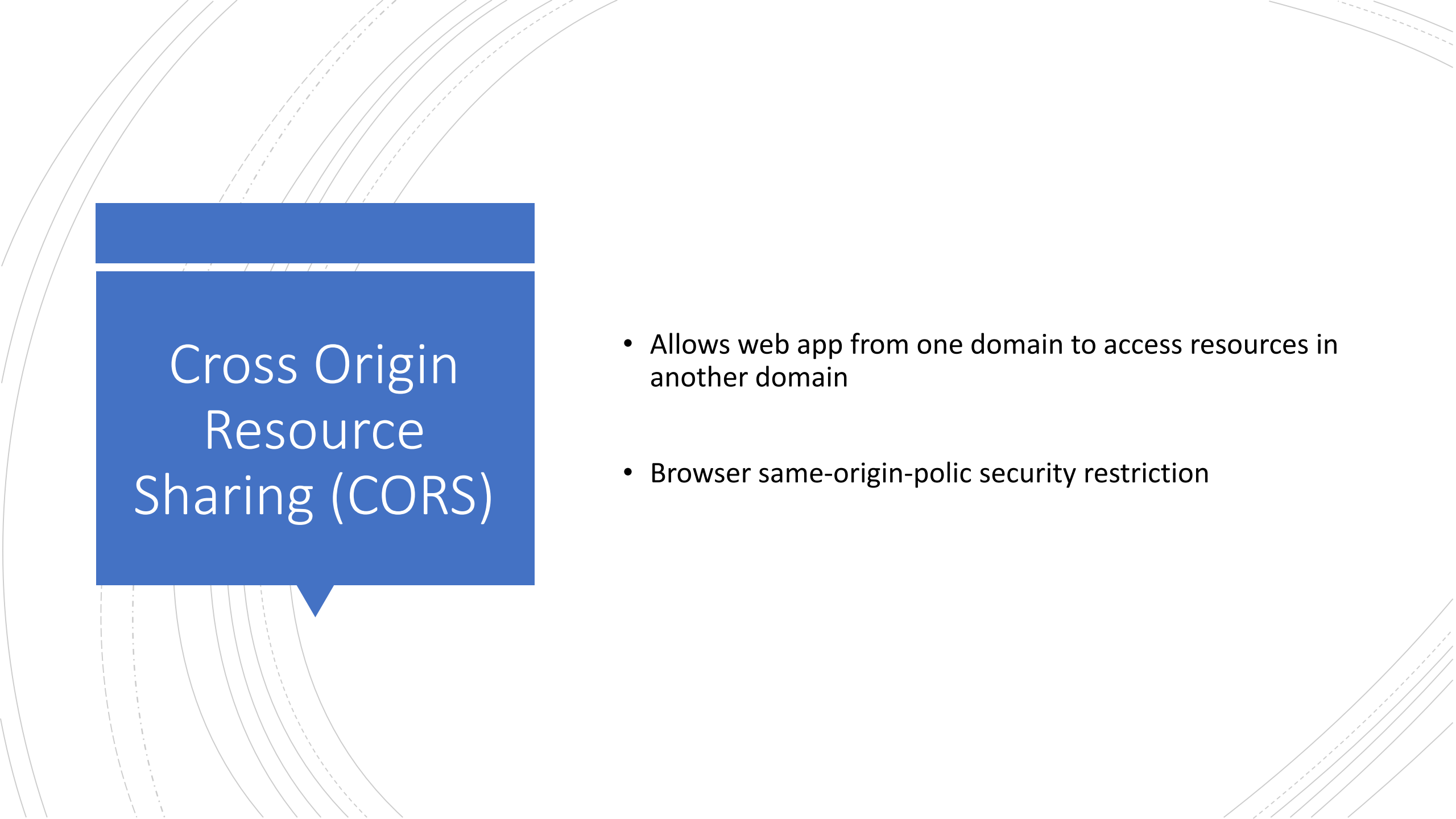
- **Ignore query strings:** Default mode. In this mode, the CDN point-of-presence (POP) node passes the query strings from the requestor to the origin server on the first request and caches the asset. All subsequent requests for the asset that are served from the POP ignore the query strings until the cached asset expires.
- **Bypass caching for query strings:** In this mode, requests with query strings are not cached at the CDN POP node. The POP node retrieves the asset directly from the origin server and passes it to the requestor with each request.
- **Cache every unique URL:** In this mode, each request with a unique URL, including the query string, is treated as a unique asset with its own cache. For example, the response from the origin server for a request for `example.ashx?q=test1` is cached at the POP node and returned for subsequent caches with the same query string. A request for `example.ashx?q=test2` is cached as a separate asset with its own time-to-live setting.

<https://docs.microsoft.com/en-us/azure/cdn/cdn-query-string>



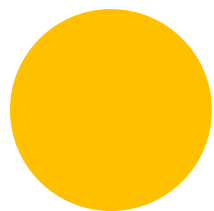
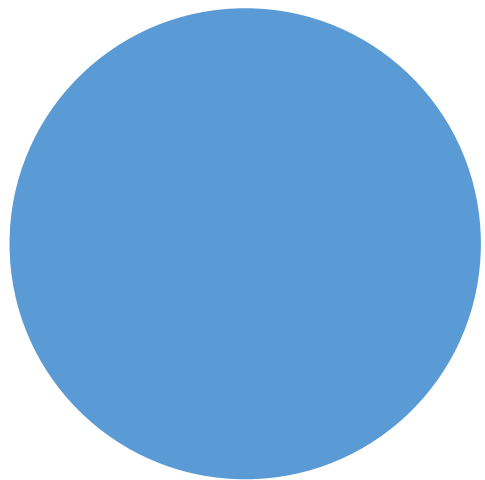
Azure CDN SSL Certificates

- Mixed content warnings
- HTTPS on custom domain
 - Azure CDN can provision and manage certificate (Verizon, Akamai)
 - Import your own certificate (Microsoft Standard pricing tier only)

The background of the slide features a series of thin, curved lines in shades of gray, creating a sense of motion and depth. These lines are more prominent on the left side and fade towards the right.

Cross Origin Resource Sharing (CORS)

- Allows web app from one domain to access resources in another domain
- Browser same-origin-policy security restriction



Azure Virtual Networks

Azure Champ

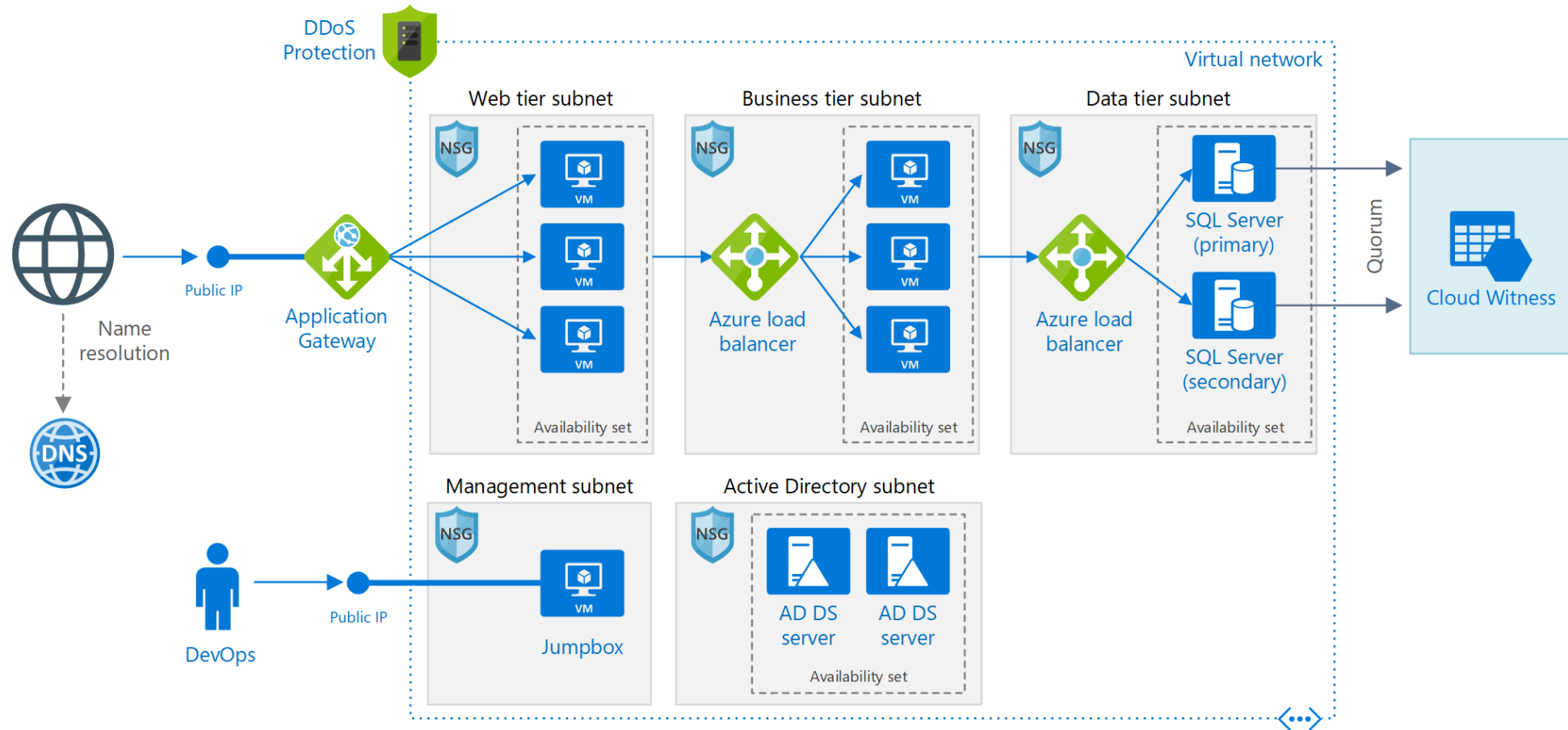


The Azure Virtual Network

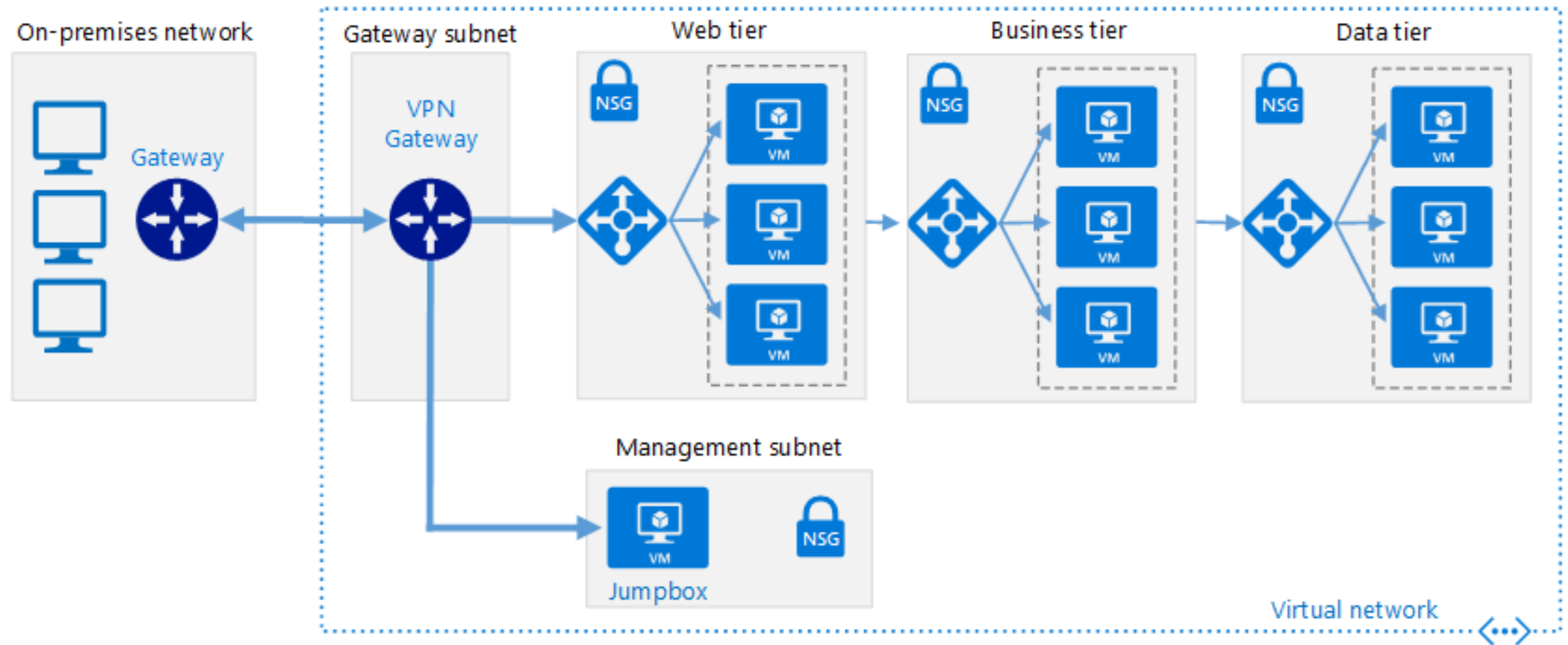
Azure Virtual Network enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

- Isolation and segmentation
- Communicate with the internet
- Communicate between Azure resources
- Communicate with on-premises resources
- Filter network traffic
- Route network traffic

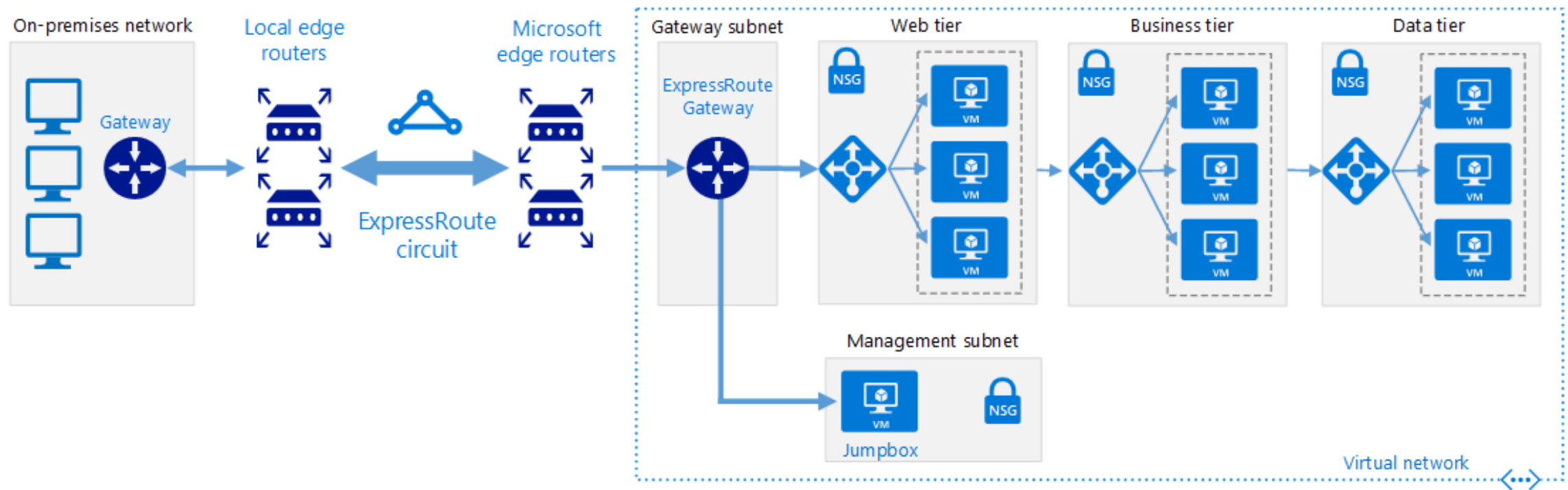
The Azure Virtual Network



The Azure Virtual Network



The Azure Virtual Network



Name Resolution for Azure vNets

- Azure-provided name resolution
- Azure DNS

Azure- provided name resolution

- No configuration required
- All VMs within a VNet can resolve each others' host names
- Problem: cross-VNet name resolution
- Problem: No custom DNS suffix
- You can add custom DNS server IP addresses
- You can host your own DNS server(s)

Azure DNS

- Host your public DNS domain in Azure
 - Use Azure geo-distributed name servers
- Create private DNS zones
 - Linked to Vnets
 - Registration Vnet
 - Resolution VNet

Azure Network Design Practices

- Design Virtual Networks
- Design IP Addressing
- Design Subnets

<https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-networking>

Design virtual networks

- Azure resources communicate privately, directly, and securely with each other over VNets.
- You can configure endpoint connections on VNets for VMs and services that require internet communication.
- A VNet is a logical isolation of the Azure cloud that's dedicated to your subscription.
- You can implement multiple VNets within each Azure subscription and Azure region.
- Each VNet is isolated from other VNets.
- VNets can contain private and public IP addresses defined in RFC 1918, expressed in CIDR notation. Public IP addresses are not directly accessible from the internet.
- VNets can connect to each other using VNet peering. Connected VNets can be in the same or different regions. Thus resources in one VNet can connect to resources in other VNets.
- By default, Azure routes traffic between subnets within a VNet, connected VNets, on-premises networks, and the internet.

Plan IP addressing

- You should assign an address space that isn't larger than a CIDR range of /16 for each VNet. VNets allow for the use of 65536 IP addresses, and assigning a smaller prefix than /16 would result in the loss of IP addresses. It's important not to waste IP addresses, even if they're in the private ranges defined by RFC 1918.
- The VNet address space shouldn't overlap with on-premises network ranges.
- Network Address Translation (NAT) shouldn't be used.
- Overlapping addresses can cause networks that can't be connected and routing that doesn't work properly. If networks overlap, you'll need to redesign the network or use network address translation (NAT).

Design subnets

- You can create multiple subnets within each VNet.
- By default, Azure routes network traffic between all subnets in a VNet.
- Your subnet decisions are based on your technical and organizational requirements.
- You create subnets using CIDR notation.
- When deciding on network range for subnets, it's important to note that Azure retains five IP addresses from each subnet that can't be used. For example, if you create the smallest available subnet of /29 (with eight IP addresses), Azure will retain **five addresses**, so you only have three usable addresses that can be assigned to hosts on the subnet.
- In most cases, using /28 as the smallest subnet is recommended.



Demo

Create Virtual Network

Network Security Groups(NSGs)

- Statefull firewall for inbound and outbound traffic
- 5 tuple hash source,destination IP and ports, protocol
- Has default rules
- Augmented rules
- Services tags and ASGs
- Bound to vNIC or Subnet



Service Tags

- A service tag represents a group of IP address prefixes to help minimize complexity for security rule creation.
- You cannot create your own service tag, nor specify which IP addresses are included within a tag.
- Microsoft manages the address prefixes encompassed by the service tag, and automatically updates the service tag as addresses change.
- You can use service tags in place of specific IP addresses when creating security rules.

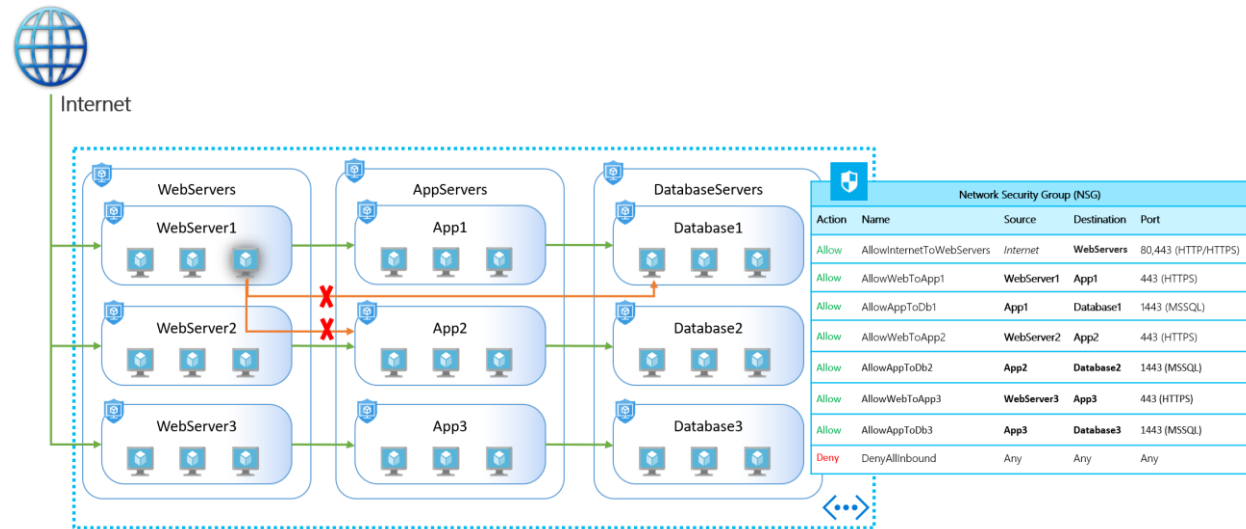
Service Tags

- Virtual Networks
- Azure Load Balancer
- Internet
- Azure Cloud
- Azure Storage
- Azure Traffic Manager
- Etc

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#service-tags>



Application Security Groups (ASGs)



- 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.



Demo

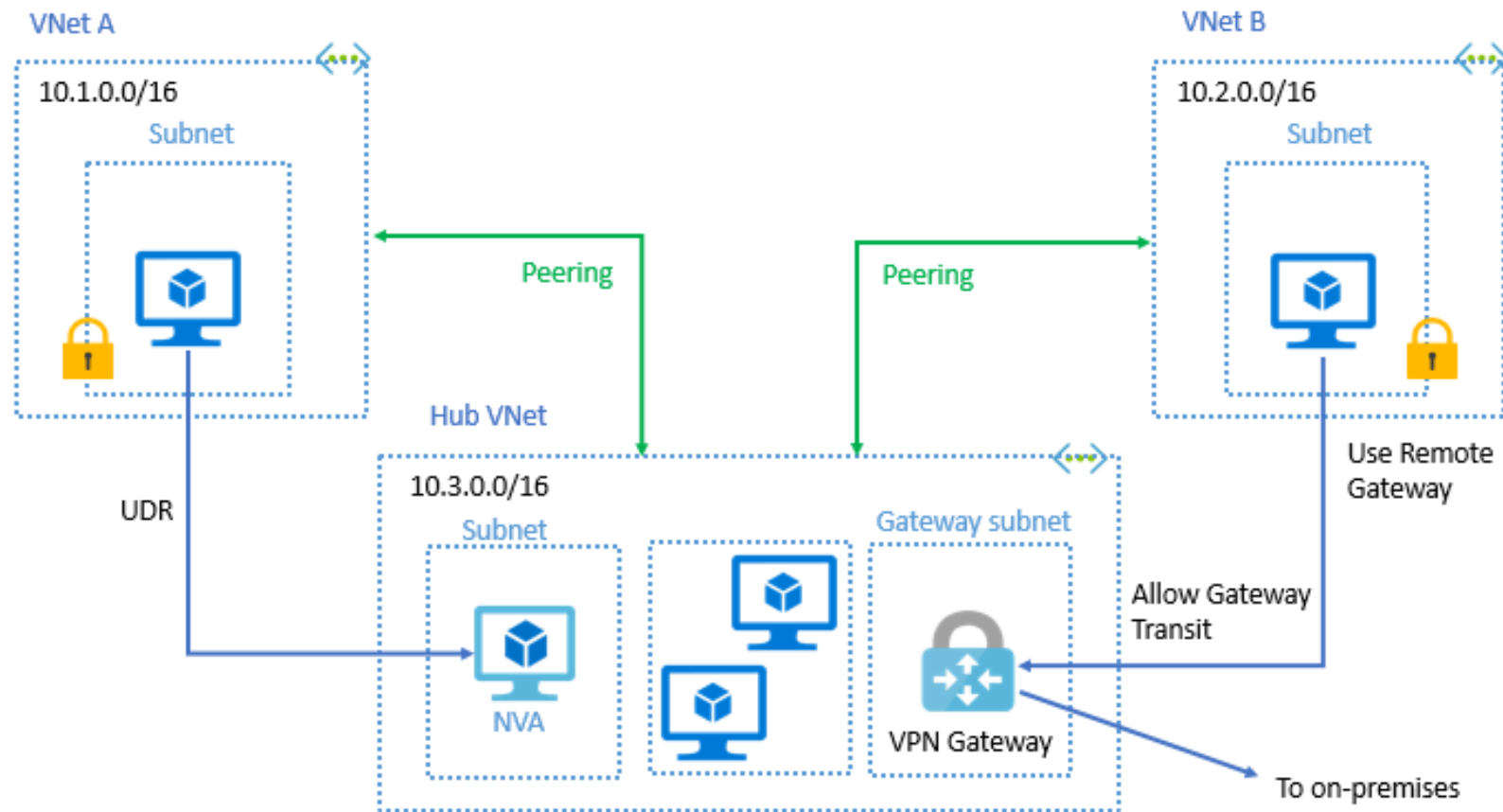
Create NSG Rule



Demo

Create vNIC

Virtual network peering



Routing Network Traffic

- System routes

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	172.16.0.0/12	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

How Azure Selects a Route

1. User-defined Route
2. BGP Route
3. System Route





Demo

Custom Routing

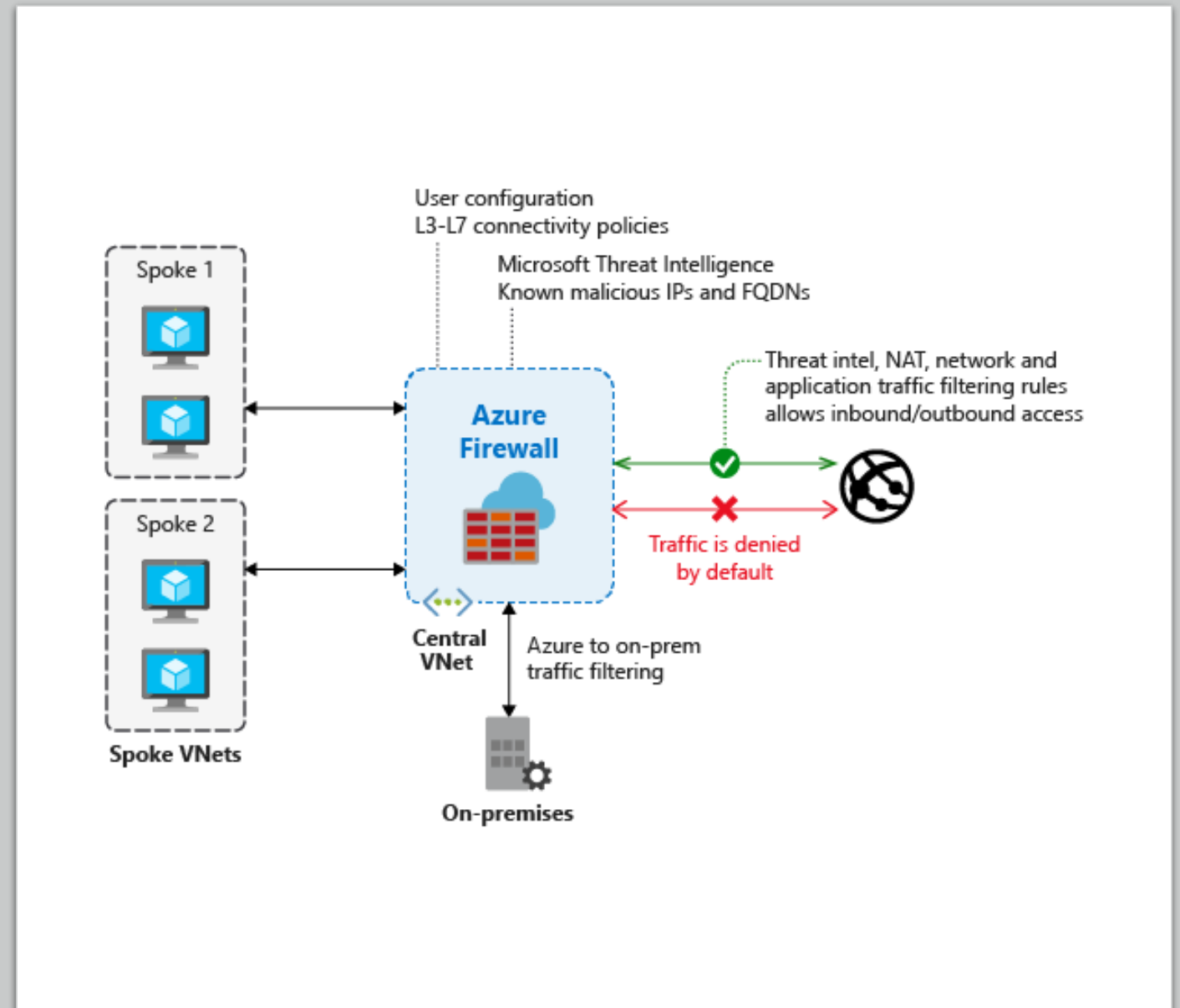
Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.

It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

Azure Firewall

- Built-in high availability
- Unrestricted cloud scalability
- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Service tags
- Threat intelligence
- Outbound SNAT support
- Inbound DNAT support
- Azure Monitor logging



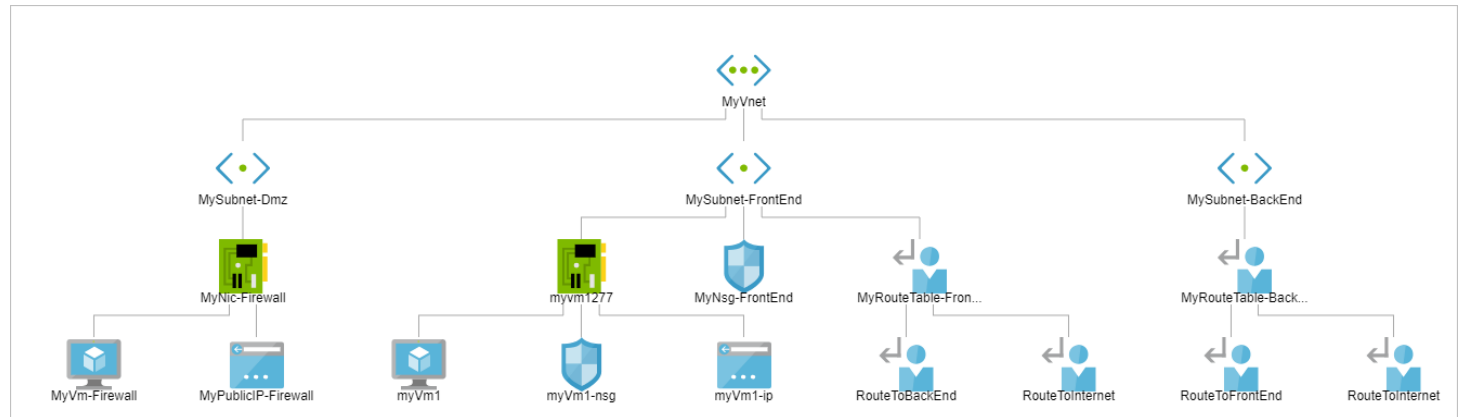


Demo

Azure Firewall

Azure Network Watcher

- Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.
- View resources in a virtual network and their relationships



Azure Network Watcher

- Diagnose network traffic filtering problems to or from a VM
- Diagnose network routing problems from a VM
- Diagnose outbound connections from a VM
- Capture packets to and from a VM
- Diagnose problems with an Azure Virtual network gateway and connections
- Determine relative latencies between Azure regions and internet service providers
- View security rules for a network interface





Demo

Azure Network Watcher



Azure DNS

Azure Champ



Azure-provided name resolution

- No configuration required
- All VMs within a VNet can resolve each others' host names
- Problem: cross-VNet name resolution
- Problem: No custom DNS suffix
- You can add custom DNS server IP addresses
- You can host your own DNS server(s)

The background of the slide features a series of thin, curved lines in shades of gray, creating a sense of motion and depth. These lines are more prominent on the left side and fade towards the right.

Azure DNS

- Host your public DNS domain in Azure
 - Use Azure geo-distributed name servers
- Create private DNS zones
 - Linked to Vnets
 - Registration Vnet
 - Resolution VNet

The background of the slide features a series of concentric, curved lines in a light gray color, creating a sense of motion or a stylized globe. These lines are more prominent on the left side and fade out towards the right.

The Resolution Virtual Networks

- To publish a private DNS zone to your virtual network, you specify the list of virtual networks that are allowed to resolve records within the zone. These are called resolution virtual networks.

The Registration Virtual Network

- You may also specify a virtual network for which Azure DNS maintains hostname records whenever a VM is created, changes IP, or is deleted. This is called a registration virtual network.

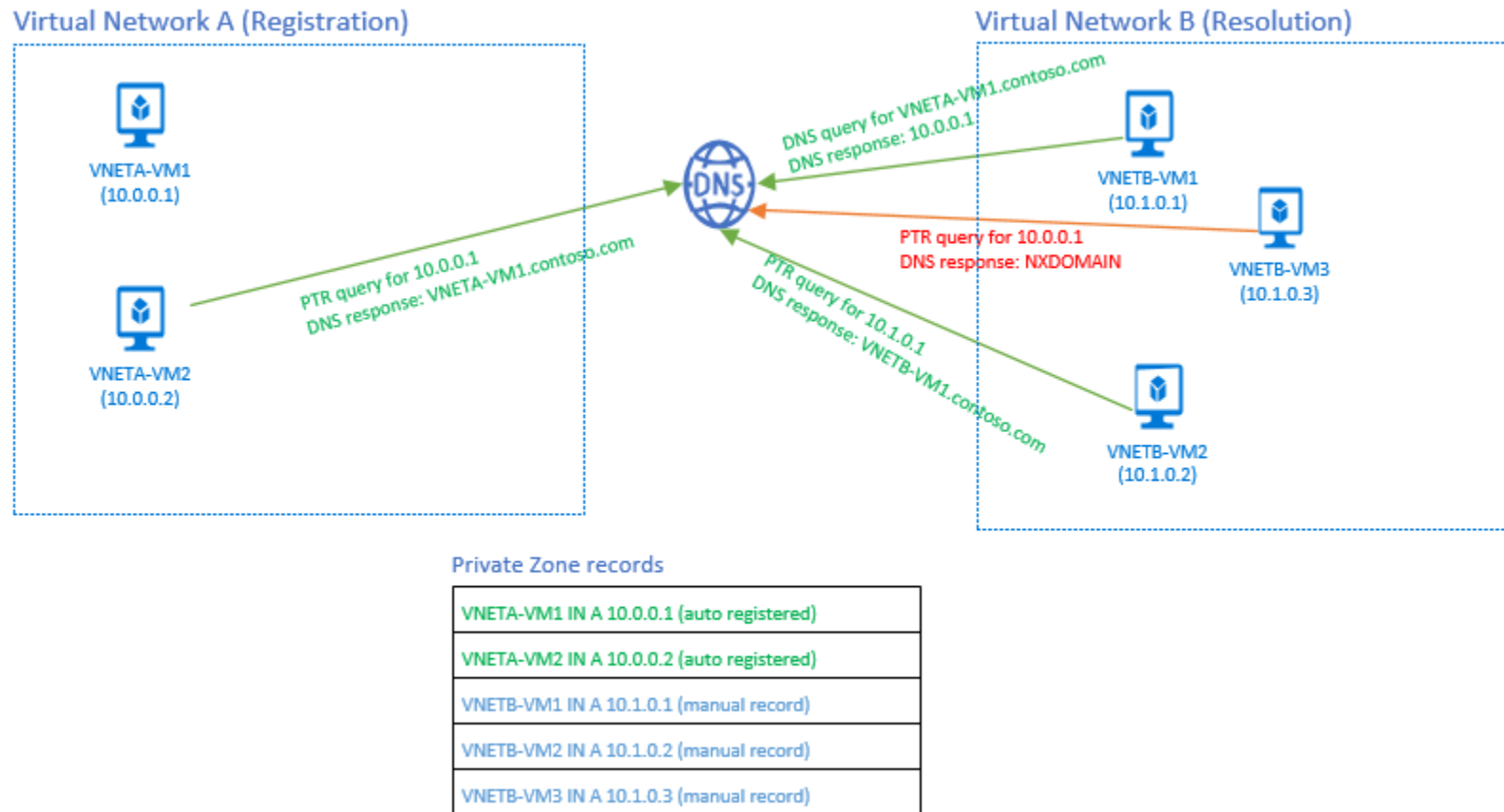
Azure Private DNS Zones Benefit

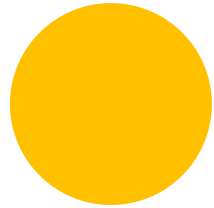
- Removes the need for custom DNS solutions. Previously, many customers created custom DNS solutions to manage DNS zones in their virtual network. You can now perform DNS zone management by using the native Azure infrastructure, which removes the burden of creating and managing custom DNS solutions.
- Use all common DNS records types. Azure DNS supports A, AAAA, CNAME, MX, PTR, SOA, SRV, and TXT records.
- Automatic hostname record management. Along with hosting your custom DNS records, Azure automatically maintains hostname records for the VMs in the specified virtual networks. In this scenario, you can optimize the domain names you use without needing to create custom DNS solutions or modify applications.
- Hostname resolution between virtual networks. Unlike Azure-provided host names, private DNS zones can be shared between virtual networks. This capability simplifies cross-network and service-discovery scenarios, such as virtual network peering.
- Familiar tools and user experience. To reduce the learning curve, this new offering uses well-established Azure DNS tools (PowerShell, Azure Resource Manager templates, and the REST API).
- Split-horizon DNS support. With Azure DNS, you can create zones with the same name that resolve to different answers from within a virtual network and from the public internet. A typical scenario for split-horizon DNS is to provide a dedicated version of a service for use inside your virtual network.
- Available in all Azure regions. The Azure DNS private zones feature is available in all Azure regions in the Azure public cloud.

Azure Private DNS Zones Limitations

- Only one registration virtual network is allowed per private zone.
- Up to 10 resolution virtual networks are allowed per private zone. This limit will be removed when this feature is generally available.
- A specific virtual network can be linked to only one private zone as a registration virtual network.
- A specific virtual network can be linked to up to 10 private zones as a resolution virtual network. This limit will be removed when this feature is generally available.
- If you specify a registration virtual network, the DNS records for the VMs from that virtual network that are registered to the private zone are not viewable or retrievable from the Azure Powershell and Azure CLI APIs. The VM records are indeed registered and will resolve successfully.
- Reverse DNS works only for private IP space in the registration virtual network.
- Reverse DNS for a private IP that isn't registered in the private zone (for example, a private IP for a virtual machine in a virtual network that is linked as a resolution virtual network to a private zone) returns internal.cloudapp.net as the DNS suffix. However, this suffix isn't resolvable.
- The virtual network must be completely empty the first time you link it to a private zone as a registration or resolution virtual network. However, the virtual network can then be non-empty for future linking as a registration or resolution virtual network, to other private zones.
- Currently, conditional forwarding is not supported (for example, for enabling resolution between Azure and OnPrem networks). For information about how customers can realize this scenario via other mechanisms, see [Name resolution for VMs and role instances](#).

Azure DNS Private Zones Inter vNET Resolution





Azure Load Balancing

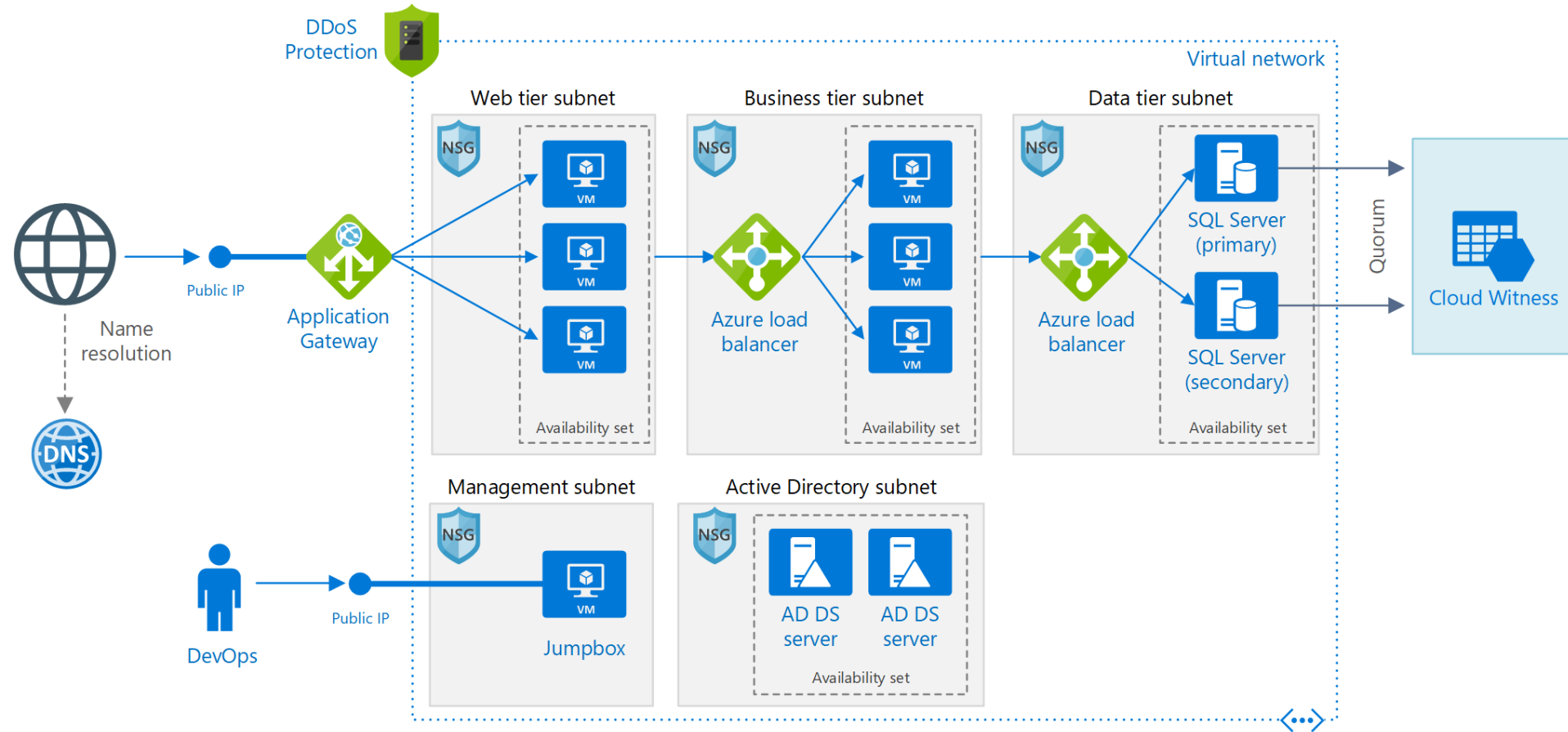
Azure Champ



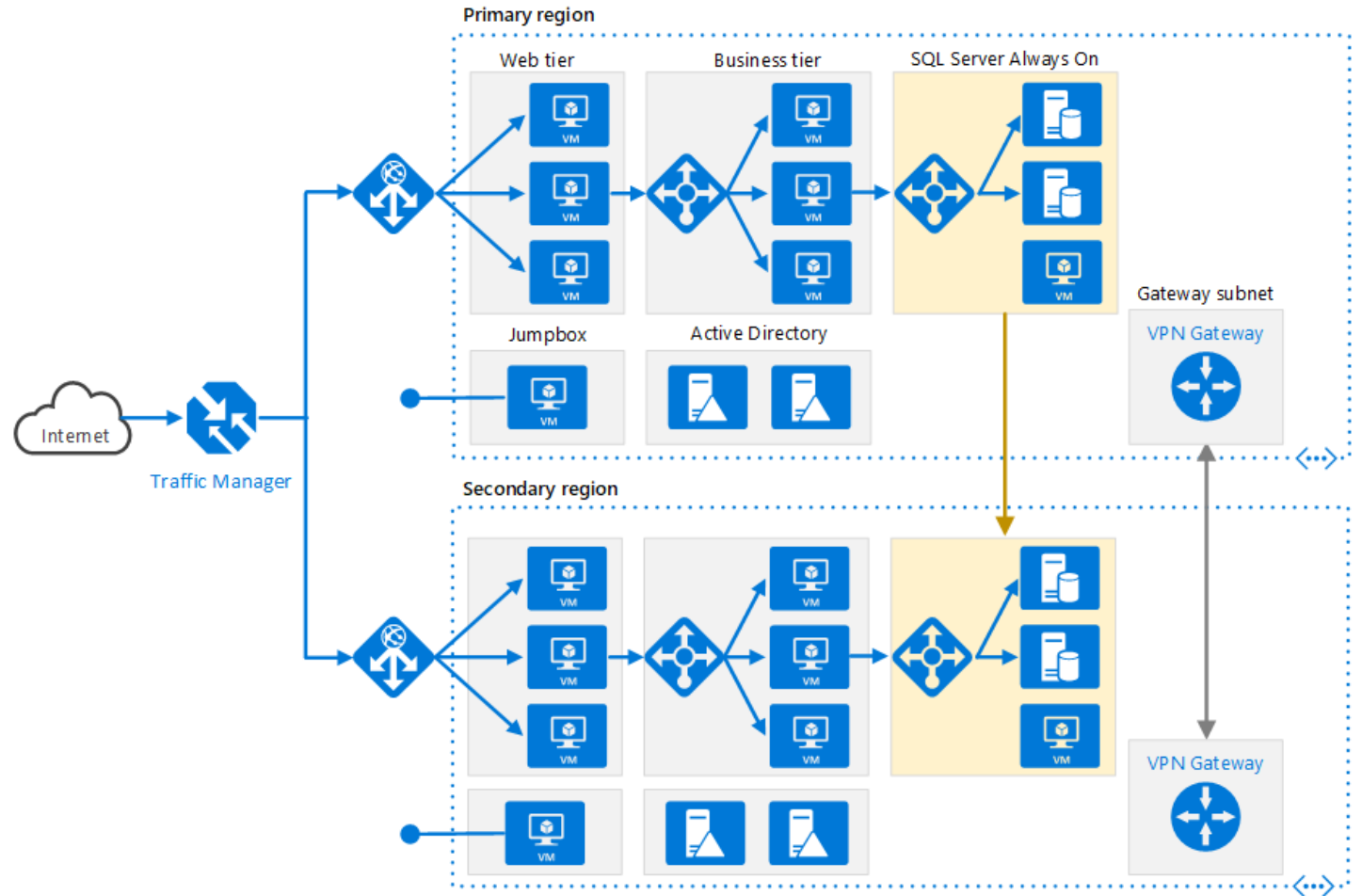
Load Balancing in Azure

Load Balancer	Application Gateway	Traffic Manager
OSI Layer 4 (TCP, UDP)	OSI Layer 7	OSI Layer 7
5-tuple Hash	SSL Offload	Global DNS Load Balancing
Load Distribution	Web Application Firewall	
Network Address Translation (NAT)		

Load Balancing in Azure



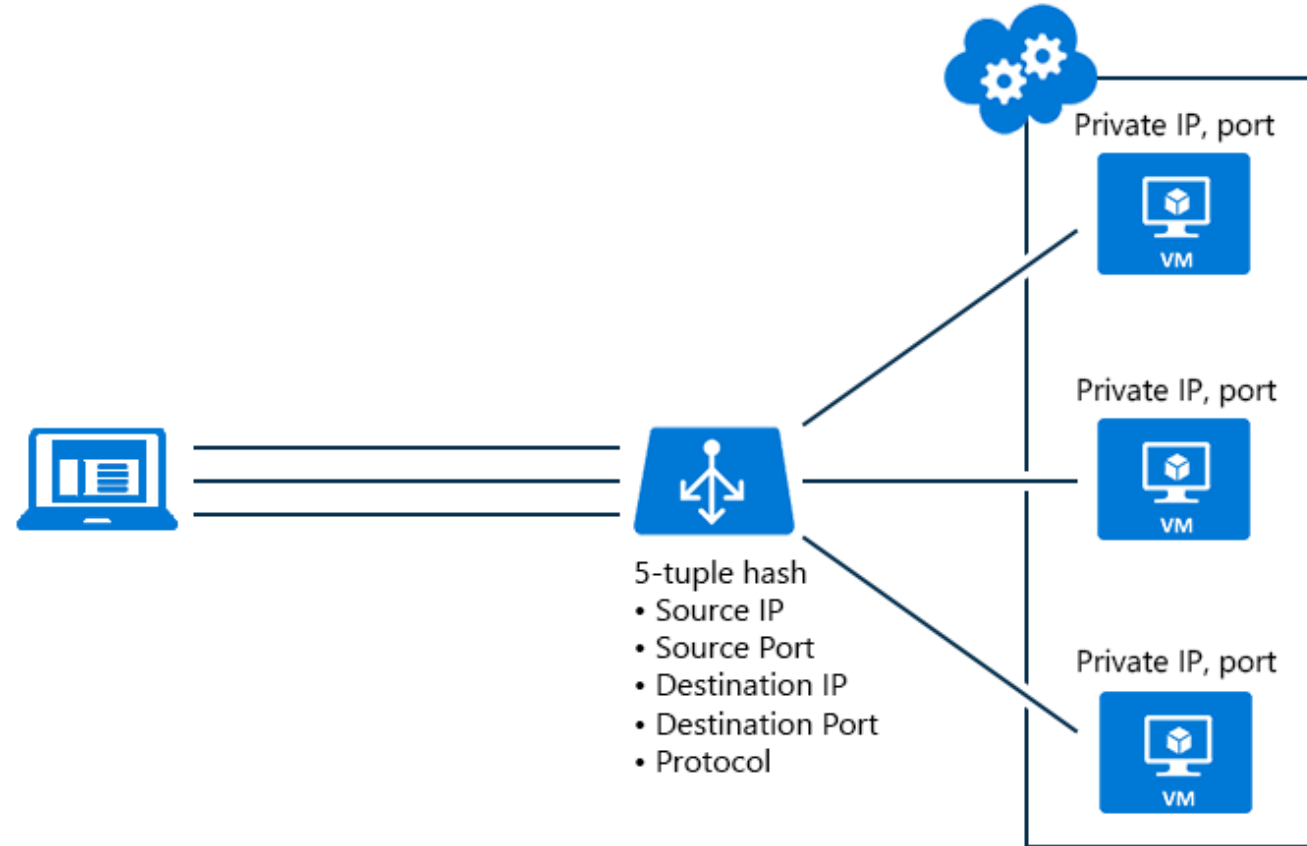
Load Balancing in Azure



Azure Public IP Address SKUs

Basic	Standard
Original PIP	New public IP tier
Dynamic or Static Allocation	Static Allocation
Open by default	Closed by default(requires NSG)
nNIC,VPN Gateway, Application Gateway, Public Load Balancer	Same resource
Not zone-redundant	Availability zone aware

Azure Load Balancer



Azure Load Balancer

- With Azure Load Balancer, you can create a load-balancing rule to distribute traffic that arrives at frontend to backend pool instances.
- Load Balancer uses a hash-based algorithm for distribution of inbound flows and rewrites the headers of flows to backend pool instances accordingly.
- Port forwarding
 - With Load Balancer, you can create an inbound NAT rule to port forward traffic from a specific port of a specific frontend IP address to a specific port of a specific backend instance inside the virtual network.
- Application agnostic and transparent
 - Load Balancer does not directly interact with TCP or UDP or the application layer, and any TCP or UDP application scenario can be supported. Load Balancer does not terminate or originate flows, interact with the payload of the flow, provides no application layer gateway function, and protocol handshakes always occur directly between the client and the backend pool instance.

Azure Load Balancer

- Automatic reconfiguration
 - Load Balancer instantly reconfigures itself when you scale instances up or down. Adding or removing VMs from the backend pool reconfigures the Load Balancer without additional operations on the Load Balancer resource.
- Health probes
 - To determine the health of instances in the backend pool, Load Balancer uses health probes that you define. When a probe fails to respond, the Load Balancer stops sending new connections to the unhealthy instances. Existing connections are not affected, and they continue until the application terminates the flow, an idle timeout occurs, or the VM is shut down.
- Outbound connections (SNAT)
 - All outbound flows from private IP addresses inside your virtual network to public IP addresses on the internet can be translated to a frontend IP address of the Load Balancer. When a public front end is tied to a backend VM by way of a load balancing rule, Azure programs outbound connections to be automatically translated to the public frontend IP address.



Demo

Azure Load Balancer

Azure Traffic Manager

- Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

Traffic Manager Routing Methods

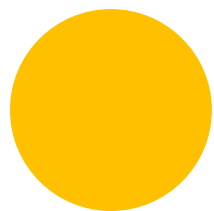
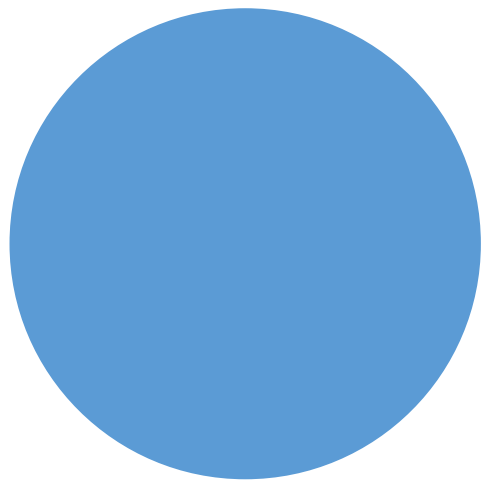
- **Priority:** Select Priority when you want to use a primary service endpoint for all traffic, and provide backups in case the primary or the backup endpoints are unavailable.
- **Weighted:** Select Weighted when you want to distribute traffic across a set of endpoints, either evenly or according to weights, which you define.
- **Performance:** Select Performance when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint in terms of the lowest network latency.
- **Geographic:** Select Geographic so that users are directed to specific endpoints (Azure, External, or Nested) based on which geographic location their DNS query originates from. This empowers Traffic Manager customers to enable scenarios where knowing a user's geographic region and routing them based on that is important. Examples include complying with data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.
- **Multivalue:** Select MultiValue for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.
- **Subnet:** Select Subnet traffic-routing method to map sets of end-user IP address ranges to a specific endpoint within a Traffic Manager profile. When a request is received, the endpoint returned will be the one mapped for that request's source IP address.





Demo

Azure Traffic Manager



Azure Hybrid Cloud

Azure Champ

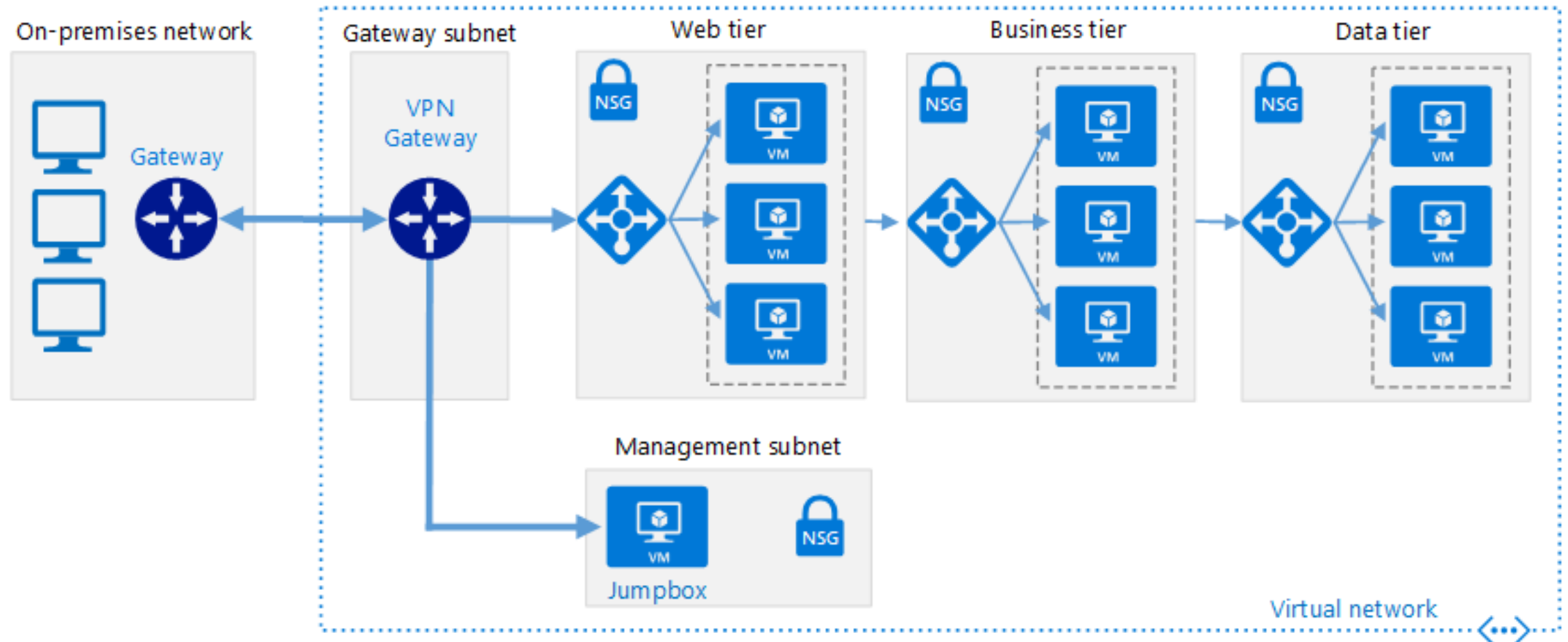


Why we need a Hybrid Cloud?

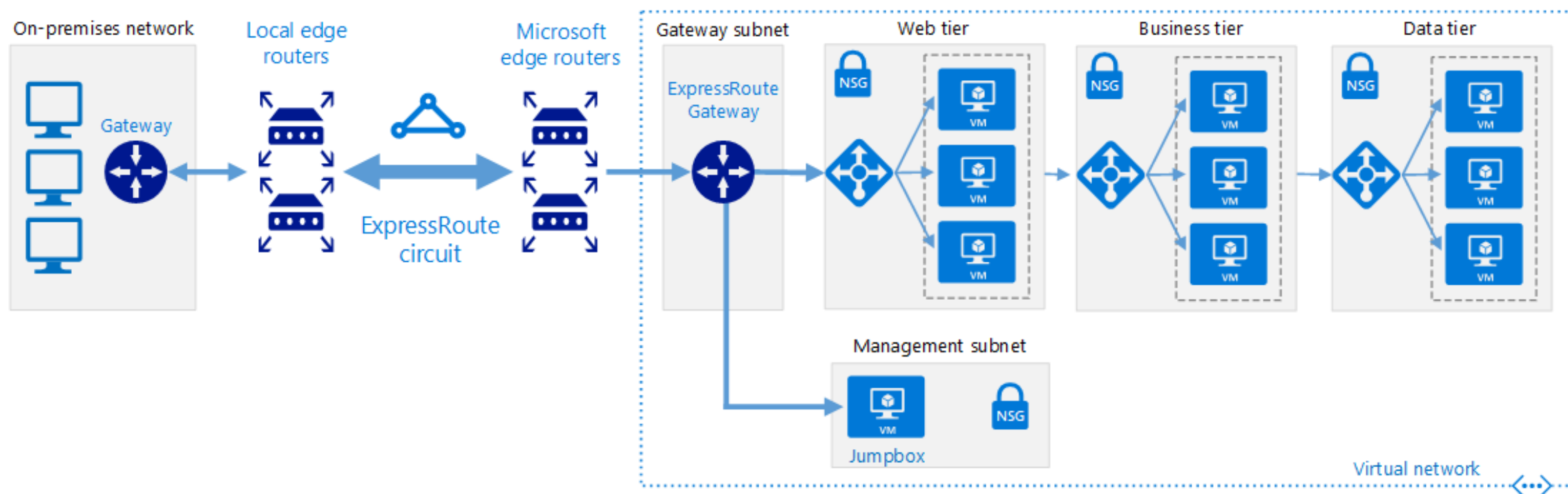
- Deploy mission critical Workloads to Azure.
- Manage on-premises from Azure.
- Azure as a Disaster site, Backup.
- Secure WAN cloud for branch offices.
- Local regulations.



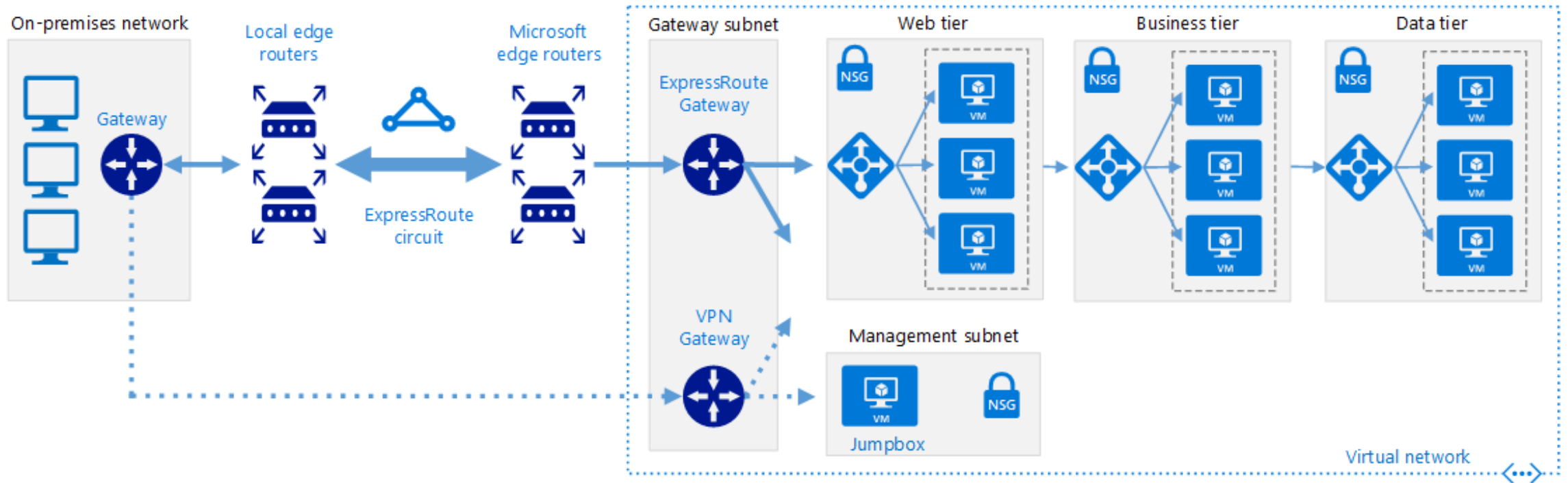
Site to Site VPN



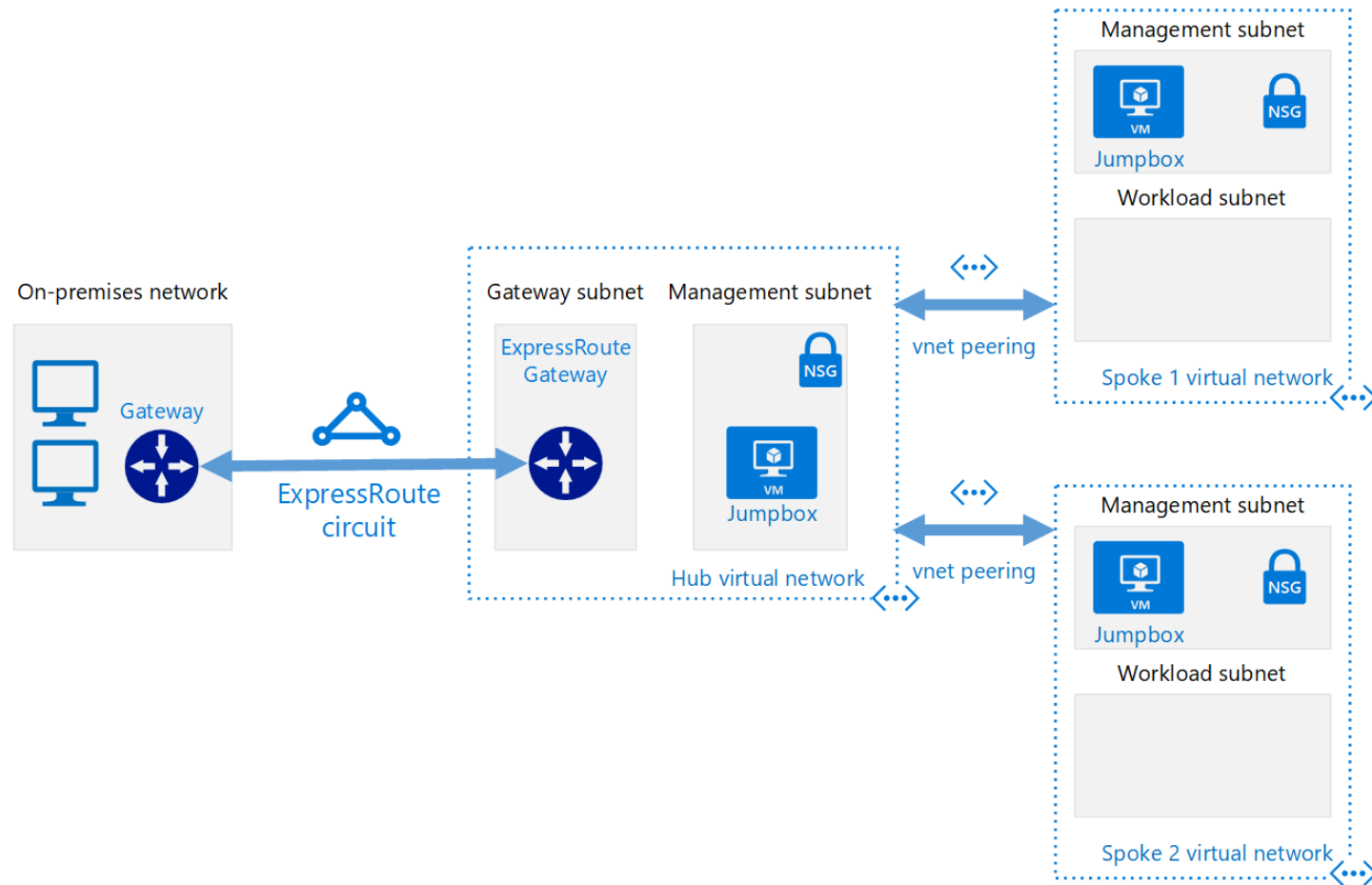
Express Route



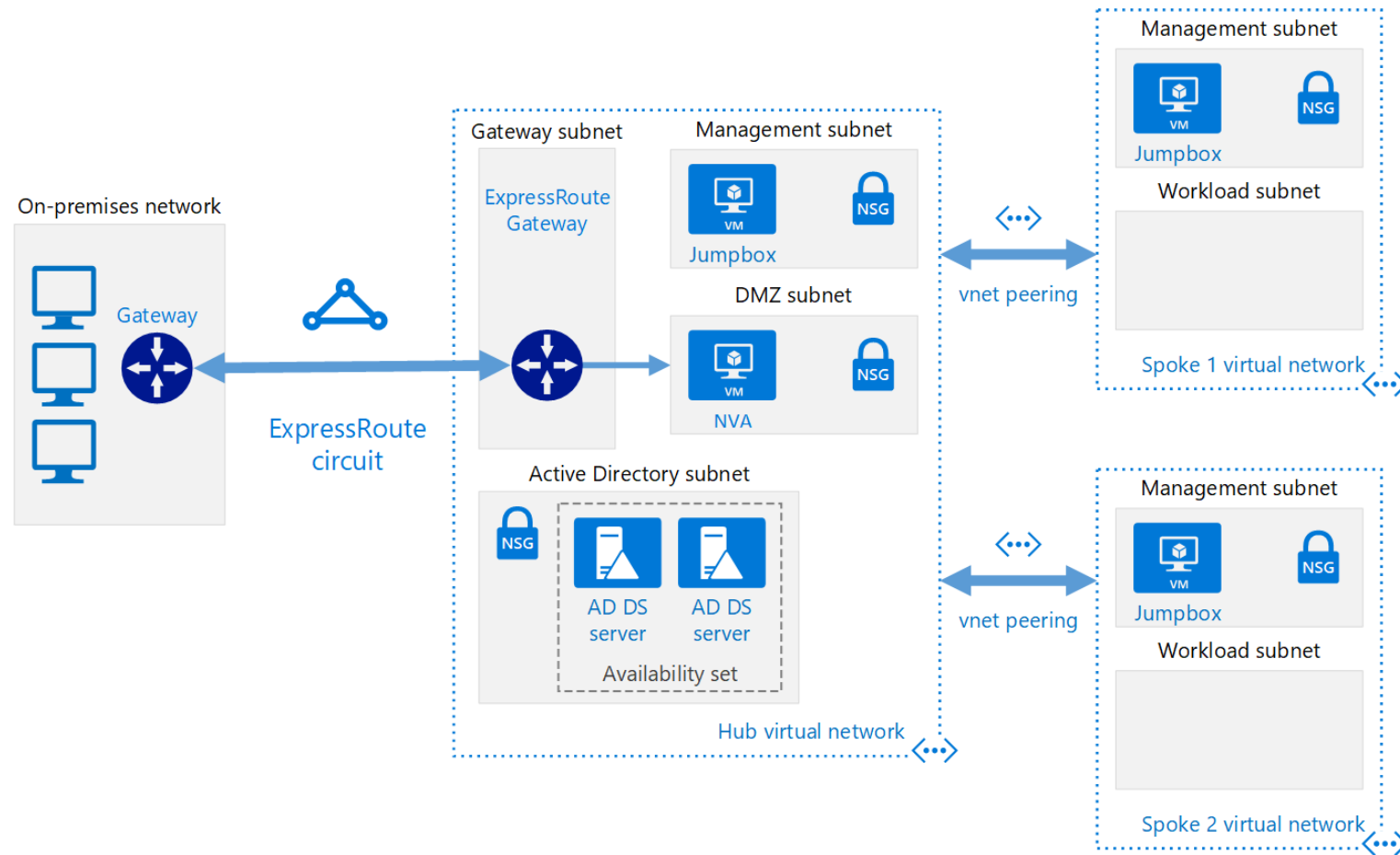
Express Route with VPN Failover



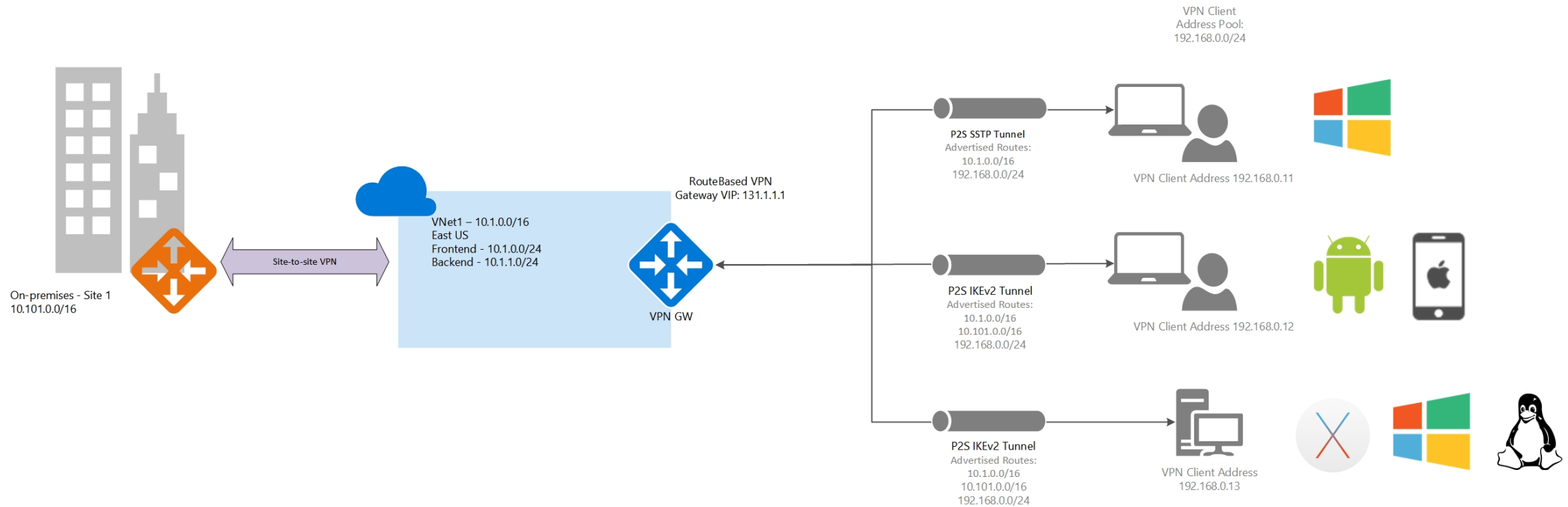
Hub and Spoke Topology



Hub and Spoke with Shared Services



Azure Point to Site VPN



Azure VPN Gateway

- For site to site VPN
 - With onprem network
 - Vnet to Vnet
- Point to Site VPN
- Express Route Circuit

Azure VPN Gateway

- Policy based gateway uses static routing
- Route based gateway uses dynamic routing

Azure VPN Gateway SKUs

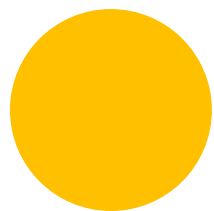
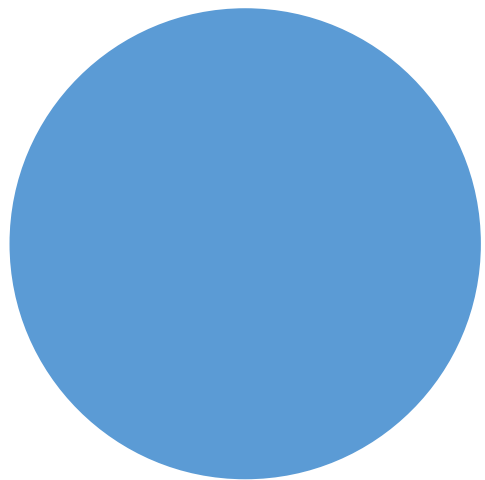
Gateway SKUs by tunnel, connection, and throughput

SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2 Connections	Aggregate Throughput Benchmark	BGP
Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported
VpnGw1	Max. 30*	Max. 128	Max. 250	650 Mbps	Supported
VpnGw2	Max. 30*	Max. 128	Max. 500	1 Gbps	Supported
VpnGw3	Max. 30*	Max. 128	Max. 1000	1.25 Gbps	Supported



Demo

Azure VPN



Azure Files

Azure Champ



What is Azure Files

- Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol.
- Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS.
- Additionally, Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.



Why Azure Files?

Azure Files Provides an Azure Storage based SMB Solution

SMB 2.1 and 3 supported

File REST Protocol Supported

Benefits

- SLA %99.9
- Availability
- Redudancy
- Disaster Recovery

Use Cases

- Cloud Native Applications
- Cross Platform Storage
- Hybrid Cloud

Azure Files Limits

500 TB Storage Account

5 TB File Share

1 TB Max file Size

1000 IOPS per share

60 MBps Throughput

%99.9 read Access to data SLA

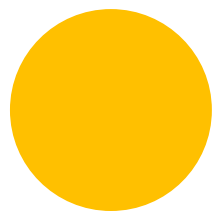
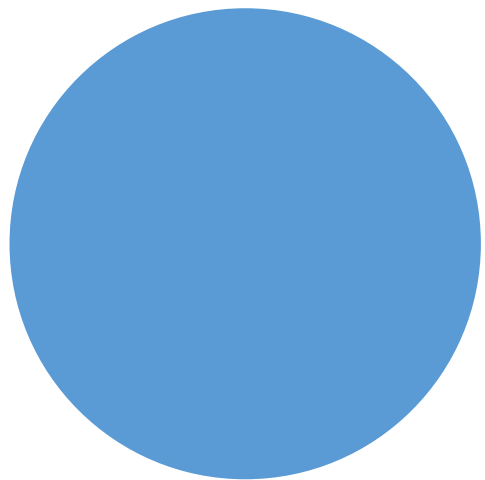
200 snapshots per share

Azure Backup Integration



Demo

Azure Files



Azure File Sync

Azure Champ



Azure File Sync

- Enables replication from single Azure Files share to one or more Windows based file servers.
- Utilize an agent deployed on each Windows Server instance that is then registered with the Storage Sync Service added to sync group.
- Cloud tiering enables infrequently accessed data to be stored in the cloud leaving thumbprint on the local server providing transparent Access.

Azure File Server Considerations

- Triggering File Recall
 - Antivirus Scan
 - Backups
- ACLs
 - Replicated to Cloud but not Enforced



Azure File Sync Limits

- 15 storage sync per subscription
- 30 Sync group per storage service
- 1 Cloud endpoint and 50 server endpoints per sync group
- 4 TB maximum space
- 100 GB maximum file size
- 64 KB minimum file size to be tiered

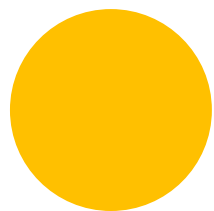
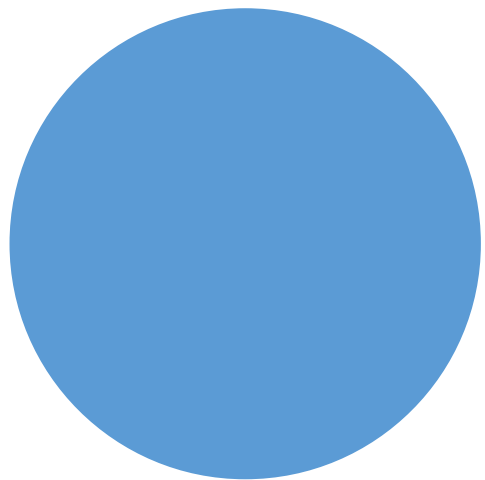
<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-scale-targets>





Demo

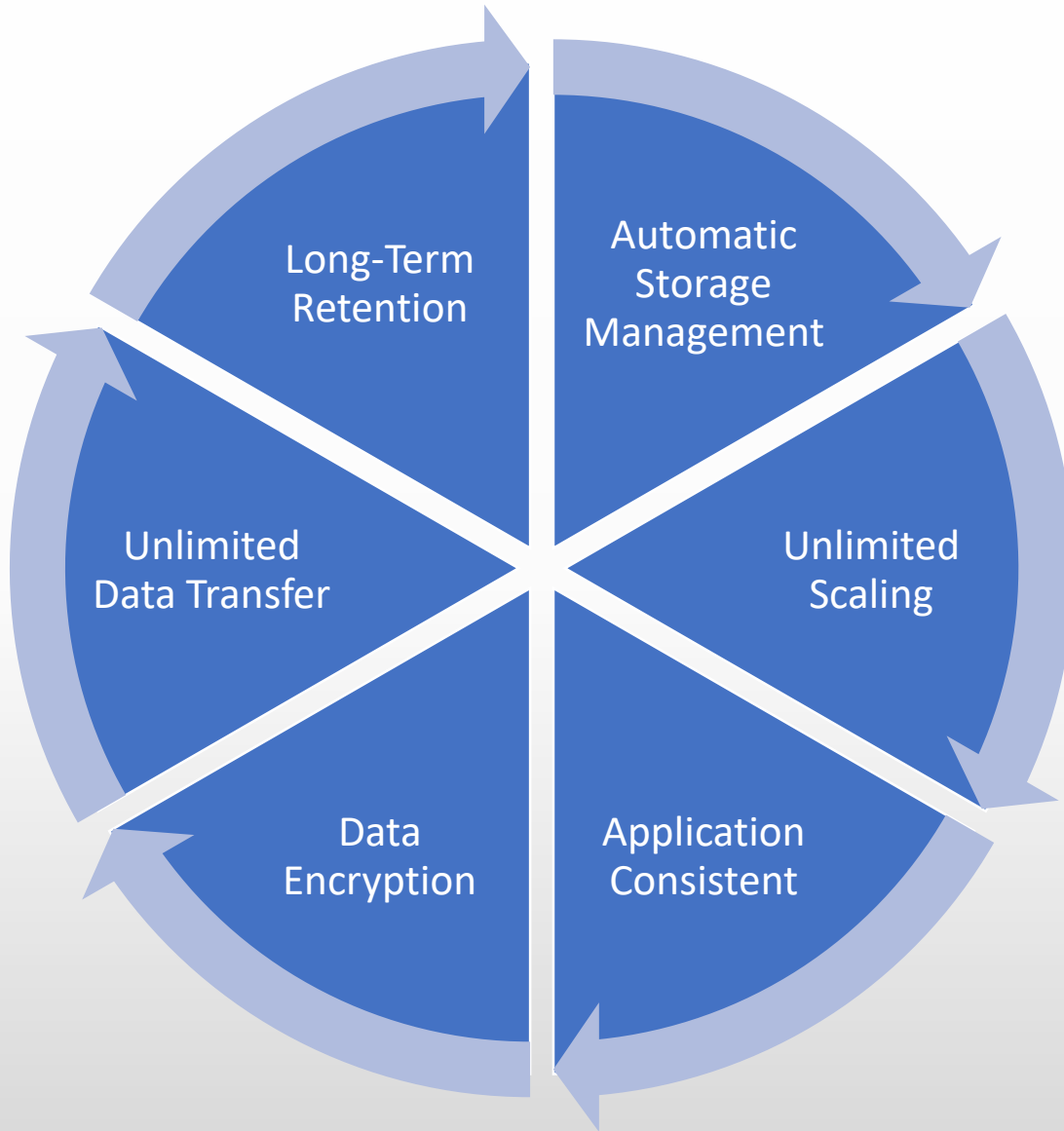
Azure File Sync



Azure Backup

Azure Champ





Azure Backup

Azure Backup Components

- Microsoft Azure IaaS VM Backup
- Microsoft Azure Backup Agent
- Microsoft Azure Backup Server

Microsoft Azure IaaS VM Backup

- Policy Driven Backup and Retention
 - Scheduled and ondemand backups, multiple recovery points
- Application Consistent Backup
 - No impact on production environment and no shutdown of VMs
- Multiple Backups Concurrently, Centralized management, detailed tracking, easy restore

Microsoft Azure Backup Agent

- Backup on-premises computers to Azure
 - Needs connectivity to Azure
- Same configuration and control
 - Centralized management of all on-premises backups
- Protected instance is registered with Azure
 - Secure Backup and recovery

Microsoft Backup Server

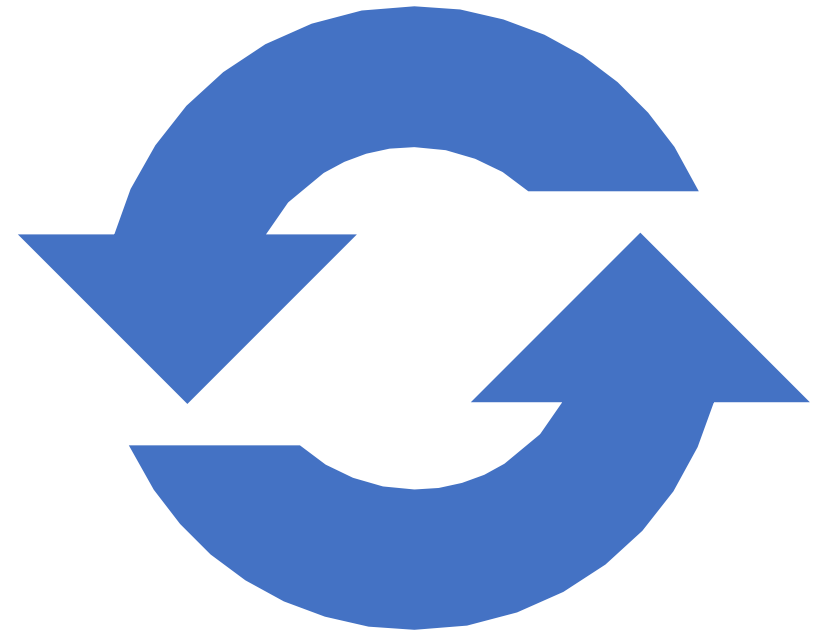
- Installed on a server in Azure or on-premises
 - Centralized Installation
- It is free
- Backup variety of instances

Recovery Services Vault

- Online storage entity in Azure used to hold data such as backup, copies, recovery points, and backup policies.

Configuring a Backup and Retention Policy

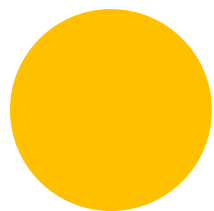
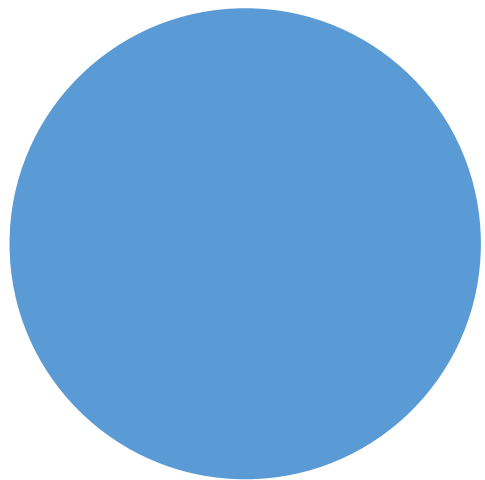
- Decide the policy type
- Backup frequency
- Retention: Daily, weekly, monthly, yearly





Demo

Azure Backup



Azure Site Recovery

Azure Champ



Azure Site Recovery

- ASR is a replication and orchestration engine

Why Use Azure Site Recovery

- Use Azure as a recovery site
- Migrate to Azure (from onprem, other cloud vendors etc.)
- Hyper-V, VMWare P2V Migration

Azure Paired Regions

<https://docs.microsoft.com/tr-tr/azure/best-practices-availability-paired-regions>

Geography	Paired regions	
North America	North Central US	South Central US
North America	East US	West US
North America	US East 2	US Central
North America	West US 2	West Central US
Europe	North Europe	West Europe
Asia	South East Asia	East Asia
China	East China	North China
Japan	Japan East	Japan West
Brazil	Brazil South (1)	South Central US
Australia	Australia East	Australia Southeast
US Government	US Gov Iowa	US Gov Virginia
India	Central India	South India
Canada	Canada Central	Canada East
UK	UK West	UK South

ASR Network Mapping

- Network mapping provides a default behavior for target network selection based on source network at the time of enabling replication.
- Retain IP addresses during failover
 - By default, when you enable disaster recovery for Azure VMs, Site Recovery creates target resources based on source resource settings. For Azure VMs configured with static IP addresses, Site Recovery tries to provision the same IP address for the target VM, if it's not in use. For a full explanation of how Site Recovery handles addressing, review this [article](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-retain-ip-azure-vm-failover).
 - For simple applications, the default configuration is sufficient. For more complex apps, you might need to provision additional resource to make sure that connectivity works as expected after failover.

<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-retain-ip-azure-vm-failover>



Recovery Plans

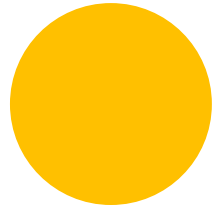
- A recovery plan gathers machines into recovery groups. You can customize a plan by adding order, instructions, and tasks to it. After a plan is defined, you can run a failover on it.





Demo

Azure Site Recovery



Azure Active Directory

Azure Champ



Azure Active Directory

Cloud based and Geo distributed

Multi tenant

Identity and Access

Azure and Office 365

Integrated with Local AD

Provide SSO

Azure Active Directory Components

Tenant

Domains

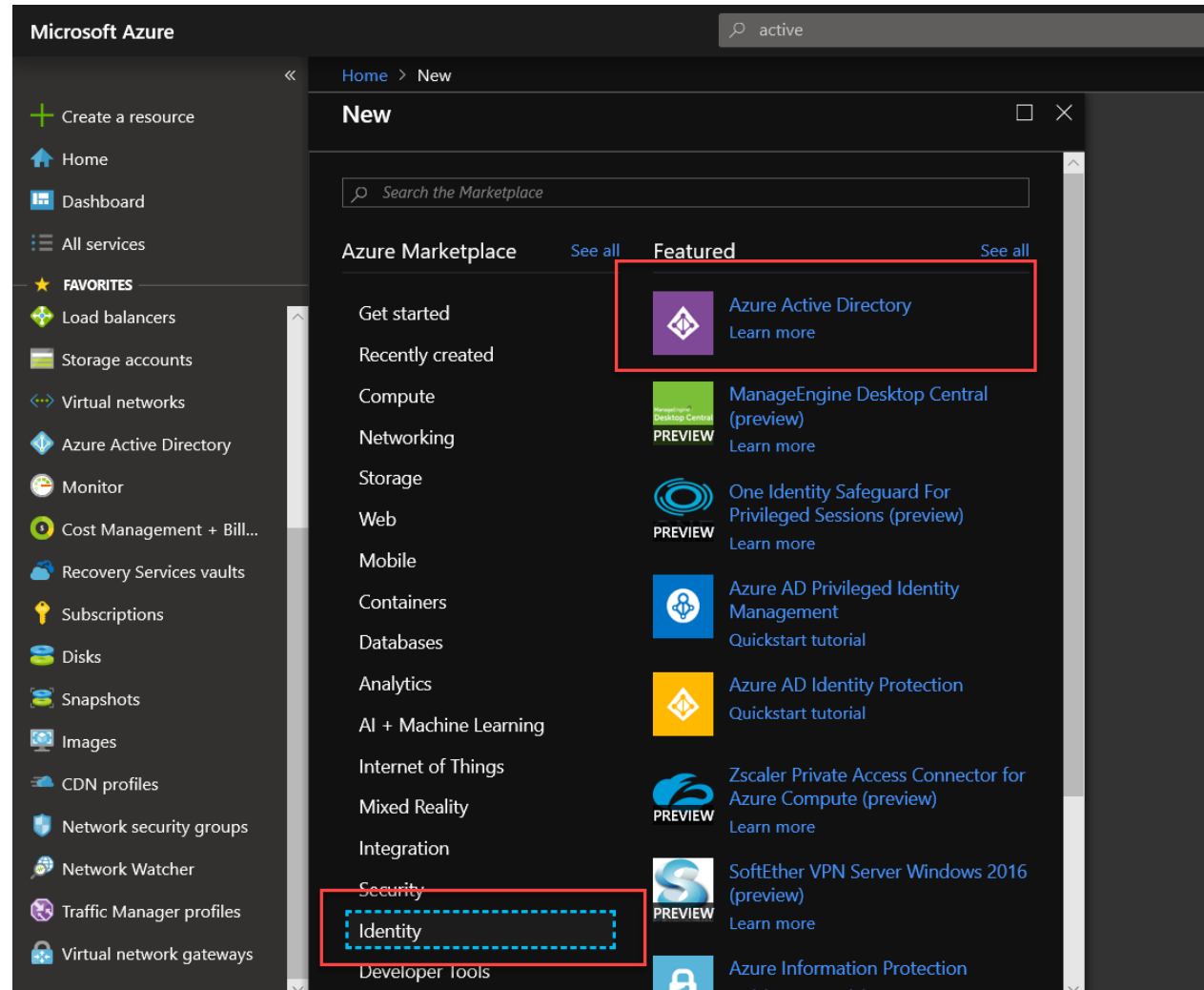
Users

Groups

Apps

Devices

Create Azure AD Tenant





Demo

Create an Azure AD Tenant

Create Azure Subscription

Home > Subscriptions

Subscriptions

Microsoft

[+ Add](#)

Showing subscriptions in Microsoft. Don't see a subscription? [Switch directories](#)

My role ⓘ

0 selected

[Apply](#)

☒ Show only subscriptions selected in the [global subscriptions filter](#) ⓘ

Search to filter items...

Status ⓘ

0 selected

← → ↻ 🏠 <https://portal.azure.com/>

Microsoft Azure

Subscription

- RESOURCES 0 results
- RESOURCE GROUPS 0 results
- SERVICES
- Subscriptions**
- FAVORITES

[+ Create a resource](#)

[All services](#)



Demo

Create a new Azure Subscription

Azure AD Comparison

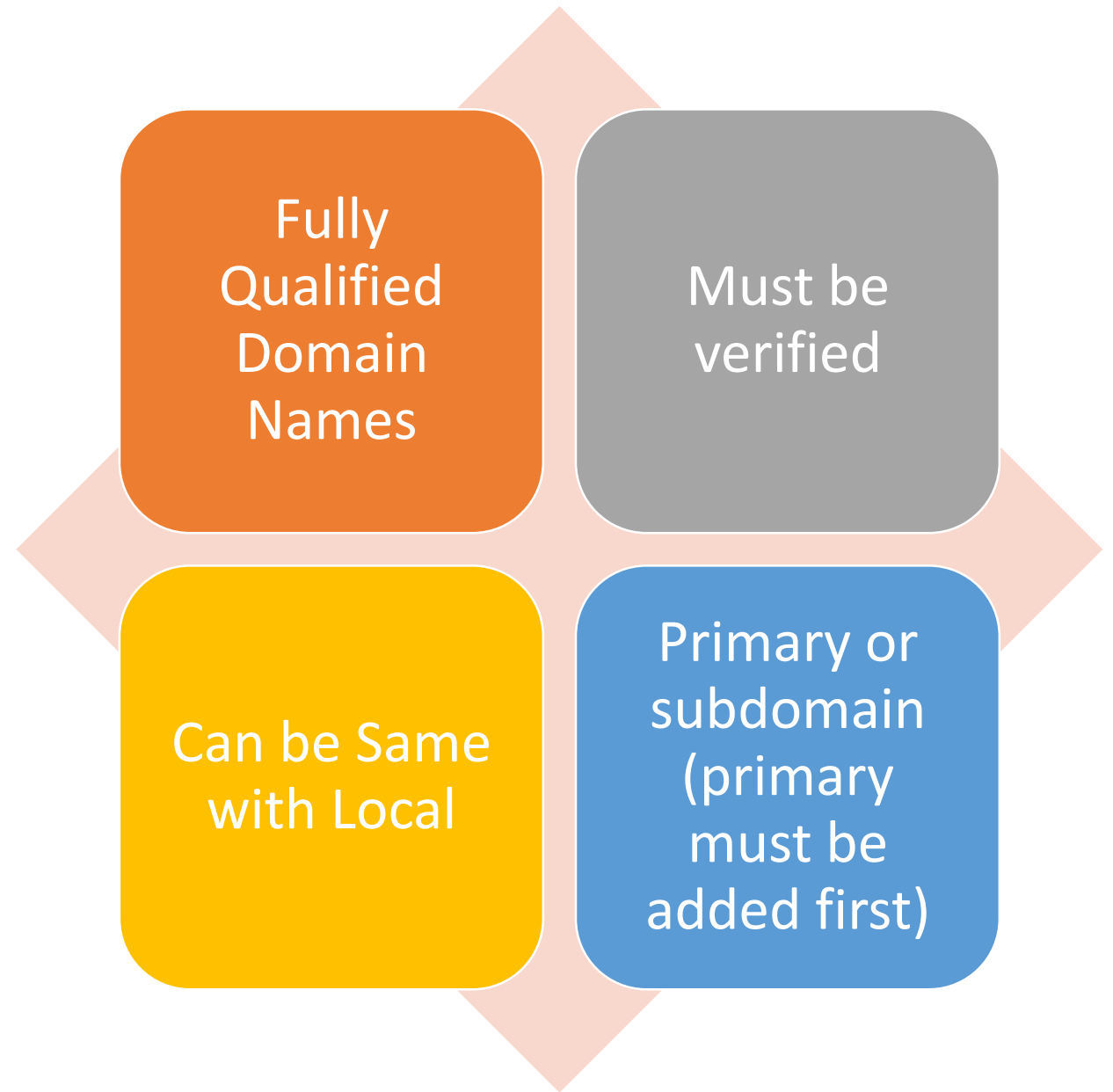
Azure Active Directory	Local Active Directory
Multi Tenant	Single Tenant
Perimeter free	Perimeter based
Flat structure	x.500 Structure
DNS Based Domains	DNS for objects
AD Graph API for queries	LDAP for queries
SAML, Oauth, WS-Federation for Authentication	Kerberos for Authentication
No OU, No Group Policy	OUs and Group Policy



Demo

Connect Azure AD

Custom Domains





Demo

Azure AD Custom Domains

Associate or add
an Azure
subscription to
your Azure
Active Directory
tenant

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and the user profile 'admin@contoso.com'. The main content area is titled 'Subscriptions' and 'Microsoft Azure Enterprise'. On the left, there is a sidebar with navigation links: 'Create a resource', 'All services', 'FAVORITES', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', 'Azure Active Directory', 'Security Center', 'Cost Management + Billing', and 'Help + support'. The central pane displays a table of subscriptions with columns 'SUBSCRIPTION ID' and 'SUBSCRIPTION NAME'. The right pane shows the details for the 'Microsoft Azure Enterprise' subscription, including 'Subscription ID', 'Directory', 'My role', 'Offer', 'Offer ID', 'Subscription name', 'Current billing period', 'Currency', and 'Status'. The 'Change directory' link is highlighted with a red box.

Microsoft Azure

Search resources, services, and docs

admin@contoso.com

Home > Subscriptions > Microsoft Azure Enterprise

Subscriptions

Microsoft

+ Add

Showing subscriptions in Microsoft. Don't see a subscription? [Switch directories](#)

My role: 7 selected Status: 3 selected

Apply

☒ Show only subscriptions selected in the global subscriptions filter

Search to filter items...

SUBSCRIPTION ID	SUBSCRIPTION NAME
XXXXX...	XXXXXXXX-XXXX ...
XXXXX...	XXXXXXXX-XXXX ...
XXXXX...	XXXXXXXX-XXXX ...
XXXXX...	XXXXXXXX-XXXX ...

Microsoft Azure Enterprise

Subscription

Search (Ctrl+/)

Manage Transfer Cancel subscription Rename **Change directory**

Subscription ID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Subscription name: [Microsoft Azure Enterprise](#)

Directory: Microsoft (microsoft.onmicrosoft.com)

Current billing period: 8/22/2018-9/21/2018

My role: Account admin

Currency: USD

Offer: MSDN

Status: Active

Offer ID: MS-AZR-0063P

For more cost management and optimization capabilities, try Azure Cost Management

Costs

Costs by resource

Company Branding

The screenshot displays the Microsoft Azure portal interface. On the left is a dark sidebar with navigation options: 'Create a resource', 'All services', 'FAVORITES', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Virtual machines', 'Azure Active Directory', 'Security Center', 'Cost Management + Billing', and 'Help + support'. The 'Azure Active Directory' option is selected. The main content area shows the breadcrumb path 'Home > Contoso - Company branding > Configure company branding'. Below this is the 'Contoso - Company branding' header with 'Azure Active Directory' as a sub-header. A search bar is present. A 'Configure' button, marked with an information icon, is highlighted with a red rectangular box. Below the button, the status is 'STATUS: Not configured'. An information icon is followed by the text: 'Configure the text and graphics your users see when they sign in to Azure Active Directory.' A list of management options is shown on the left: Overview, Getting started, Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, and Company branding (which is highlighted in blue).

Azure AD Roles

- Azure AD administrator roles are used to manage Azure AD resources in a directory such as create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains. The following table describes a few of the more important Azure AD administrator roles.

AzureAD Admin Roles vs RBAC

Azure RBAC roles

Manage access to Azure resources

Supports custom roles

Scope can be specified at multiple levels (management group, subscription, resource group, resource)

Role information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API

Azure AD administrator roles

Manage access to Azure Active Directory resources

Cannot create your own roles


Scope is at the tenant level


Role information can be accessed in Azure admin portal, Microsoft 365 admin center, Microsoft Graph, AzureAD PowerShell

Do Azure RBAC roles and Azure AD administrator roles overlap?

- By default, Azure RBAC roles and Azure AD administrator roles do not span Azure and Azure AD.
- However, if a Global Administrator elevates their access by choosing the Global admin can manage Azure Subscriptions and Management Groups switch in the Azure portal

Elevate access to manage all Azure subscriptions and management groups

 Save

 Discard

*

 Name

Default Directory

Country or region

United States


Location

United States datacenters

Notification language

English

Directory ID



Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

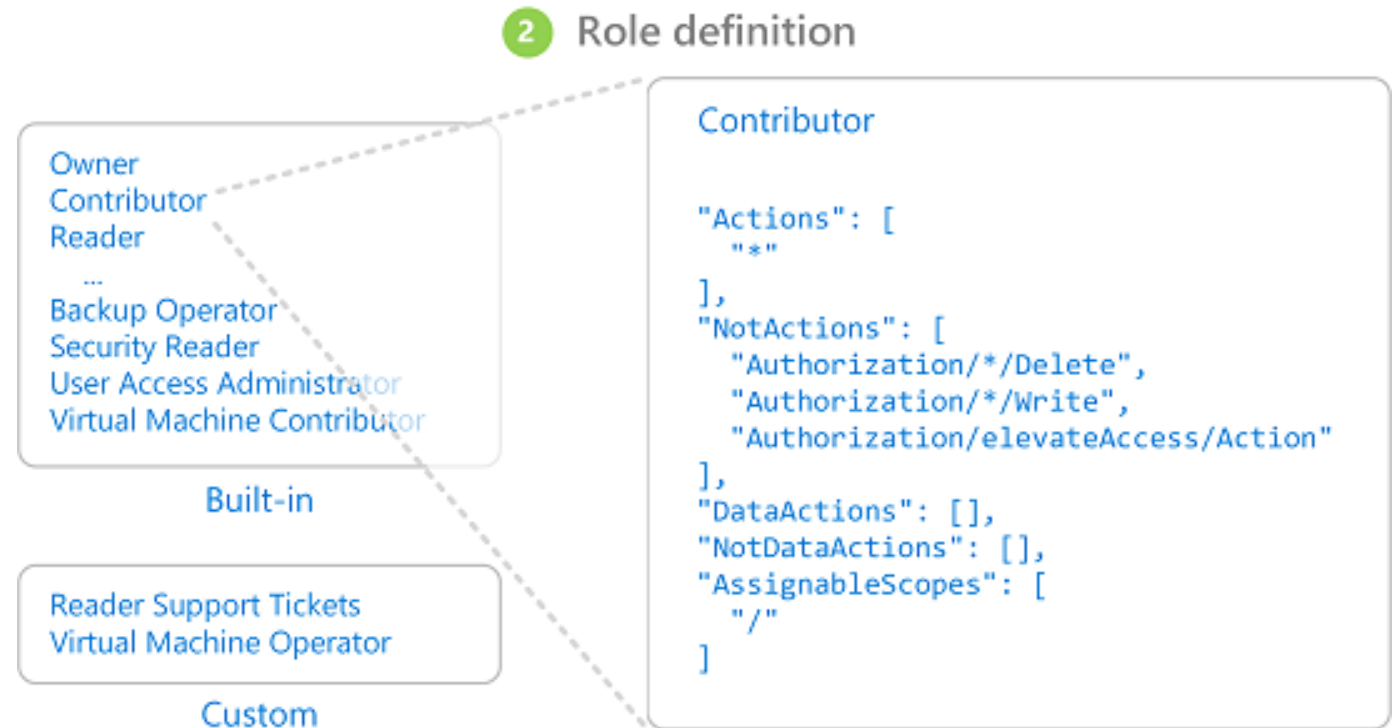
John can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes

No

Role Definitions

- A *role definition* is a collection of permissions. It's sometimes just called a *role*.
- A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine reader.





Demo

Azure AD Roles

Azure AD Users

- Cloud or Sync Users
- Member or Guest Users



Demo

Azure AD User

Azure AD Groups

- Type of Groups
 - Assigned
 - Dynamic
 - Security
 - Office 365
- Groups have owners and members
- Expiration of Groups
- Group Licenses



Demo

Azure AD Group

Self Service Password Reset

- When to use
 - Change password
 - Forgot password
 - Account lockout
- Authentication Methods
 - Text Message / Phone Call
 - Secondary Mail
 - Security Questions



Demo

Self Service Password Reset

Self Service Group Membership

- Owners can manage groups
- Users can manage groups

[Myapps.microsoft.com](https://myapps.microsoft.com)



Demo

Self Service Group Membership

Guest Users

- For business to business(B2B)
- Azure AD is not required
- Grant access to internal applications
- Document collaboration
- Conditional access supported
- Delegate to group and app owners



Demo

Guest users

Azure AD Devices

- To protect assets
- Control devices
- Standardization
- Security
- Compliance

Getting devices under the control of Azure AD

- **Registering** a device to Azure AD enables you to manage a device's identity. When a device is registered, Azure AD device registration provides the device with an identity that is used to authenticate the device when a user signs-in to Azure AD. You can use the identity to enable or disable a device.
 - When combined with a mobile device management(MDM) solution such as Microsoft Intune, the device attributes in Azure AD are updated with additional information about the device. This allows you to create conditional access rules that enforce access from devices to meet your standards for security and compliance.
- **Joining** a device is an extension to registering a device. This means, it provides you with all the benefits of registering a device and in addition to this, it also changes the local state of a device. Changing the local state enables your users to sign-in to a device using an organizational work or school account instead of a personal account.

Hybrid Azure AD joined devices

- If your environment has an on-premises AD footprint and you also want benefit from the capabilities provided by Azure Active Directory, you can implement hybrid Azure AD joined devices. These are devices that are joined to your on-premises Active Directory and registered with your Azure Active Directory.