Microsoft Azure

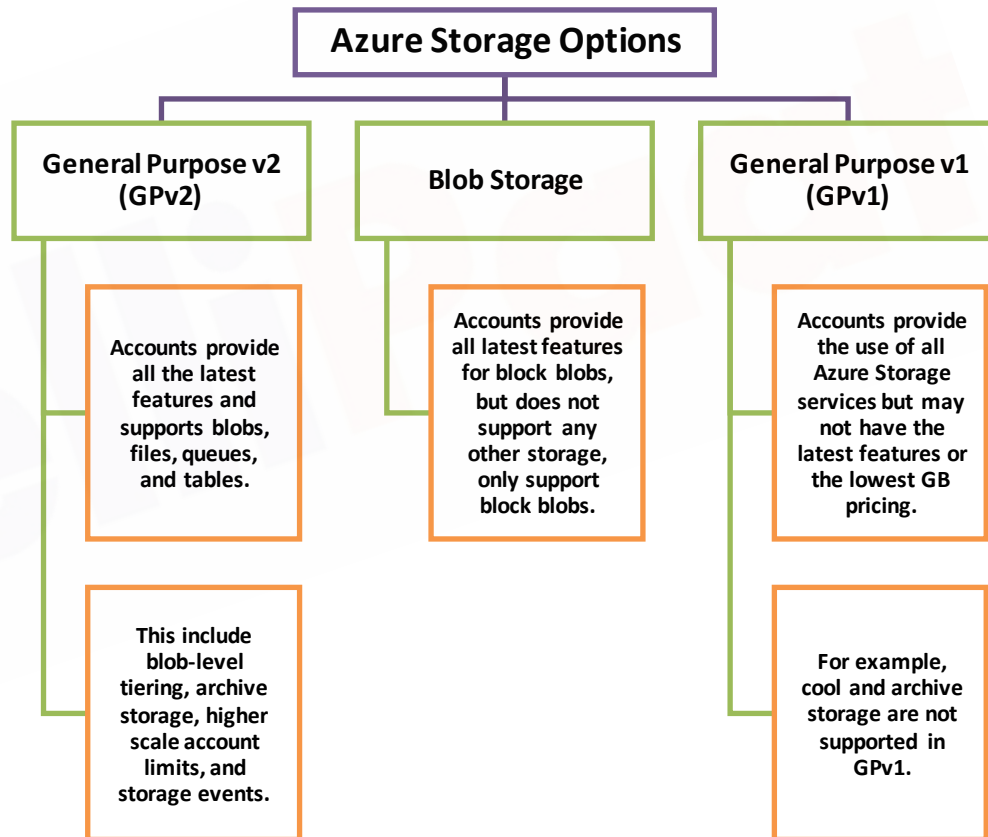# Administrator Associate Training

Implement and Manage Storage

Agenda

- Azure Storage
- Azure Blob Storage
- Azure File Storage
- Azure Table Storage
- Azure Queue Storage
- Virtual Network
- Azure DNS
- Azure AD

Azure Storage

What Is Azure Storage?

❑ Azure Storage provides storage that is highly available, secure, durable, scalable, and redundant.

❑ Azure Storage offers various data services such as:

- Blob Storage

- File Storage

- Queue Storage

- Table

Azure Storage Options

General Purpose v2 (GPv2)

Accounts provide all the latest features and supports blobs, files, queues, and tables.

This include blob-level tiering, archive storage, higher scale account limits, and storage events.

Blob Storage

Accounts provide all latest features for block blobs, but does not support any other storage, only support block blobs.

General Purpose v1 (GPv1)

Accounts provide the use of all Azure Storage services but may not have the latest features or the lowest GB pricing.

For example, cool and archive storage are not supported in GPv1.

Azure Storage:
General Purpose v2

❑ General Purpose v2 (GPv2) are storage accounts which support all features for all storage services, including blobs, files, queues, and tables.

❑ For block blobs, you can choose between hot and cool storage tiers at account level or hot, cool, and archive tiers at the blob level based on access patterns.

❑ Store frequently, infrequently, and rarely accessed data in the hot, cool, and archive storage tiers, respectively, to optimize costs.

❑ Importantly, any GPv1 account can be upgraded to a GPv2 account in the portal, CLI, or PowerShell.

Azure Storage: Pricing

❑ All storage accounts use a pricing model for blob storage based on the tier of each blob.

❑ When using a storage account, the following billing considerations apply:

Storage costs
- The cost of storing data varies depending on the storage tier.
- The per-gigabyte cost decreases as the tier gets cooler.

Data access costs
- Data access charges increase as the tier gets cooler.
- For data in the cool and archive storage tiers, you are charged a per-gigabyte data access charge for reads.

Transaction costs
- There is a per-transaction charge for all tiers.

Geo-replication data transfer costs
- This only applies to accounts with geo-replication configuration, including GRS and RA-GRS.
- Geo-replication data transfer incurs a per-gigabyte charge.
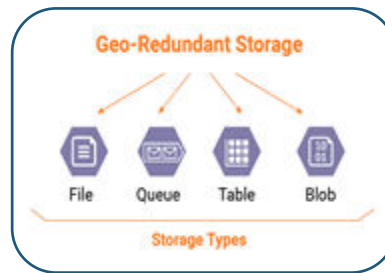
Azure Storage: Replication

❑ The data in your Microsoft Azure storage account is always replicated to ensure durability and high availability.

❑ Replication copies your data, either within the same data center or to a second data center, depending on which replication option you choose.

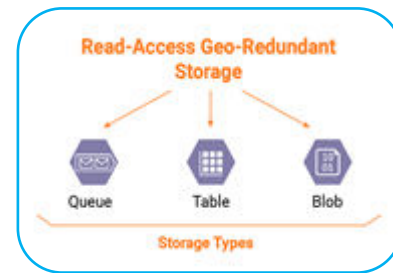❑ When you create a storage account, you can select one of the following replication options:
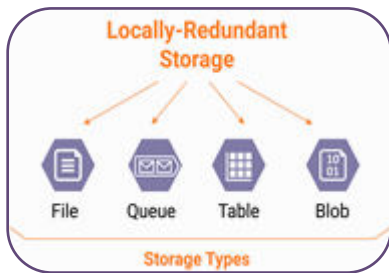
Locally-Redundant Storage (LRS)
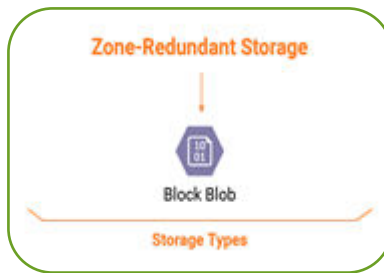
Zone-Redundant Storage (ZRS)

Geo-Redundant Storage (GRS)

Read-Access Geo-Redundant Storage (RA-GRS)

Azure Storage: Differences

Replication Strategy	LRS	ZRS	GRA	RA-GRS
Data is replicated across multiple datacenters.	No	Yes	Yes	Yes
Data can be read from a secondary location, as well as from the primary location.	No	No	No	Yes
Designed to provide durability of objects over a given year.	At least 99.999999999 % (11 9s)	At least 99.9999999999 % (12 9s)	At least 99.99999999 999999% (16 9s)	At least 99.99999999999 999% (16 9s)

Azure Storage: Tiers

Azure storage offers three storage tiers for blob object storage:

Hot Storage Tier	Cool Storage Tier	Archive Storage Tier

The Azure hot storage tier is optimized for storing data that is accessed frequently.

The Azure cool storage tier is optimized for storing data that is infrequently accessed and stored for at least 30 days.

The Azure archive storage tier is optimized for storing data that is rarely accessed and stored for at least 180 days.

Azure Storage: Security

- Azure Storage provides a comprehensive set of security capabilities.
- The storage account itself can be secured using Role-based Access Control and Azure Active Directory.
- Data can be secured in transit between an application and Azure by using Client-side Encryption, HTTPS, or SMB 3.0.
- Data can be set to be automatically encrypted when written to Azure Storage using Storage Service Encryption.
- OS and data disks used by virtual machines can be set to be encrypted using Azure Disk Encryption.
- Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures.
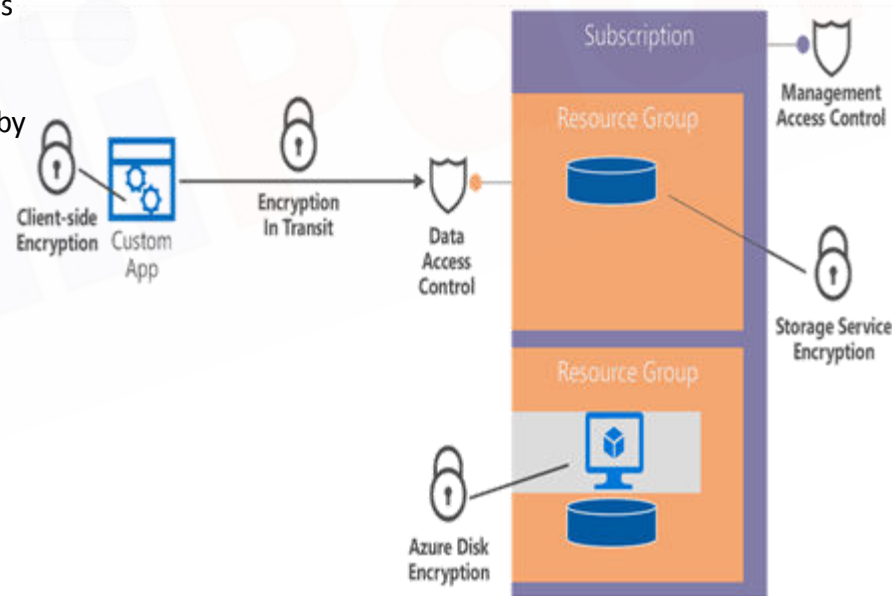
Azure Blob Storage

What Is Azure Blob Storage?

❑ Azure Blob storage is a service for storing large amounts of

unstructured object data, such as text or binary data.

❑ You can use Blob storage to expose data publicly to the world or

to store application data privately.

❑ Common uses of Blob storage include:

  o Serving images or documents directly to a browser

  o Storing files for distributed access

  o Storing data for backup and restore, disaster recovery, and archiving
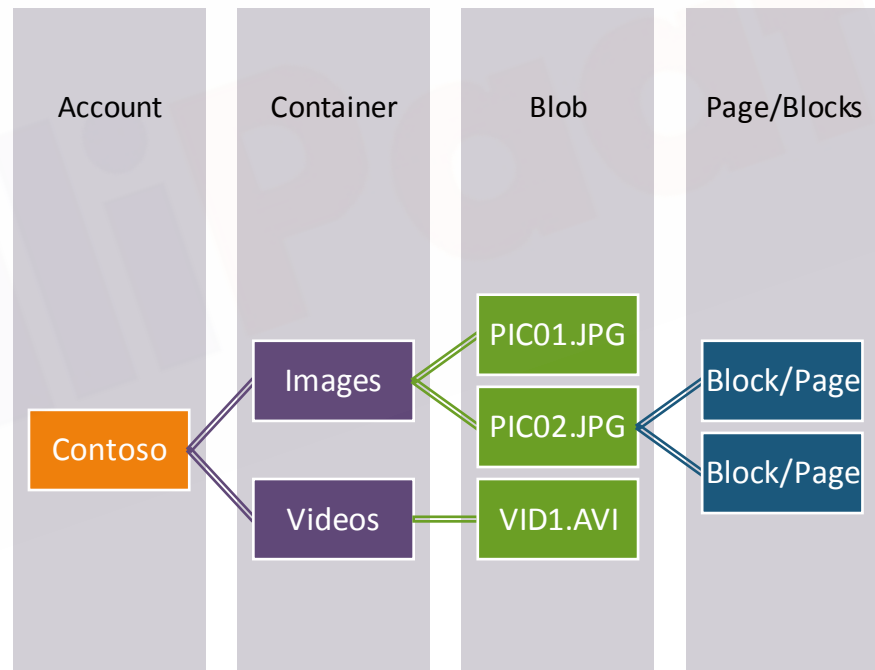
Azure Blob: Concept

❑ **Storage Account**

    ○ All access to Azure Storage is done through a storage account.

    ○ This account can be a general purpose or a Blob storage.

❑ **Container**

    ○ A container provides grouping of a set of blobs.

    ○ All blobs must be in a container.

    ○ An account can contain an unlimited number of containers.

    ○ A container can store an unlimited number of blobs.

❑ **Blob**

    ○ A file of any type and size.

    ○ Azure Storage offers three types of blobs

        ▪ **Block Blobs**

        ▪ **Page Blobs**

        ▪ **Append Blobs**

Account	Container	Blob	Page/Blocks
Contoso	Images	PIC01.JPG	Block/Page
		PIC02.JPG	Block/Page
	Videos	VID1.AVI	

Azure Blob: Types

Block Blobs

- Each block can be of a different size, up to a maximum of 100 MB.
- They are used for storing text or binary files, such as documents and media files.
- A single block blob can contain up to 50,000 blocks. Individual block blobs can be up to 4.75 TB in size (100 MB X 50,000).
- With a block blob, you can upload multiple blocks in parallel to decrease the upload time.

Append Blobs

- Each block in an append blob can be of a different size, up to a maximum of 4 MB.
- They are similar to block blobs in that they are made up of blocks, but they are optimized for append operations, so they are useful for logging scenarios.
- A single append blob can contain up to 50,000 blocks, for a total size of slightly more than 195 GB (4 MB X 50,000).

Page Blobs

- Page blobs are a collection of 512-byte pages optimized for random read and write operations.
- They can be up to 8 TB in size and are more efficient for frequent read/write operations.
- Azure virtual machines use page blobs as OS and data disks.

Azure Blob:
Container

❑ You can store blobs directly in the root container of the storage account or create custom containers for storing blobs.

❑ Users can access the blob through a unique URL.

Example:

○ "**myblob.jpg**" in a container named "**mycontainer**" in a storage account named "**myaccount**" by using the following link:

http://myaccount.blob.core.windows.net/mycontainer/myblob.jpg

Azure Blob: Access Level

When you create a container, you must give it a name and choose the level of access that you want to allow from the following options:

Private
This is the default option. The container does not allow anonymous access.

Public Blob
This option allows anonymous access to each blob within the container; however, it prevents browsing the content of the container.

In other words, it is necessary to know the full path to the target blob to access it.

Public Container
This option allows anonymous access to each blob within the container, with the ability to browse the container's content.

Azure File Storage

What Is Azure File Storage?

- ❑ Azure File offers fully managed file shares in the cloud that are accessible via the Common Internet File System (CIFS).

- ❑ 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.

- ❑ The maximum size for an Azure File share is 5 TiB.

- ❑ Azure Storage account can store multiple shares with a total of 500 TiB stored across all shares.

- ❑ Azure File supports two data redundancy options:
  - ▪ Locally redundant storage (LRS)
  - ▪ Geo-redundant storage (GRS)

Azure Files:
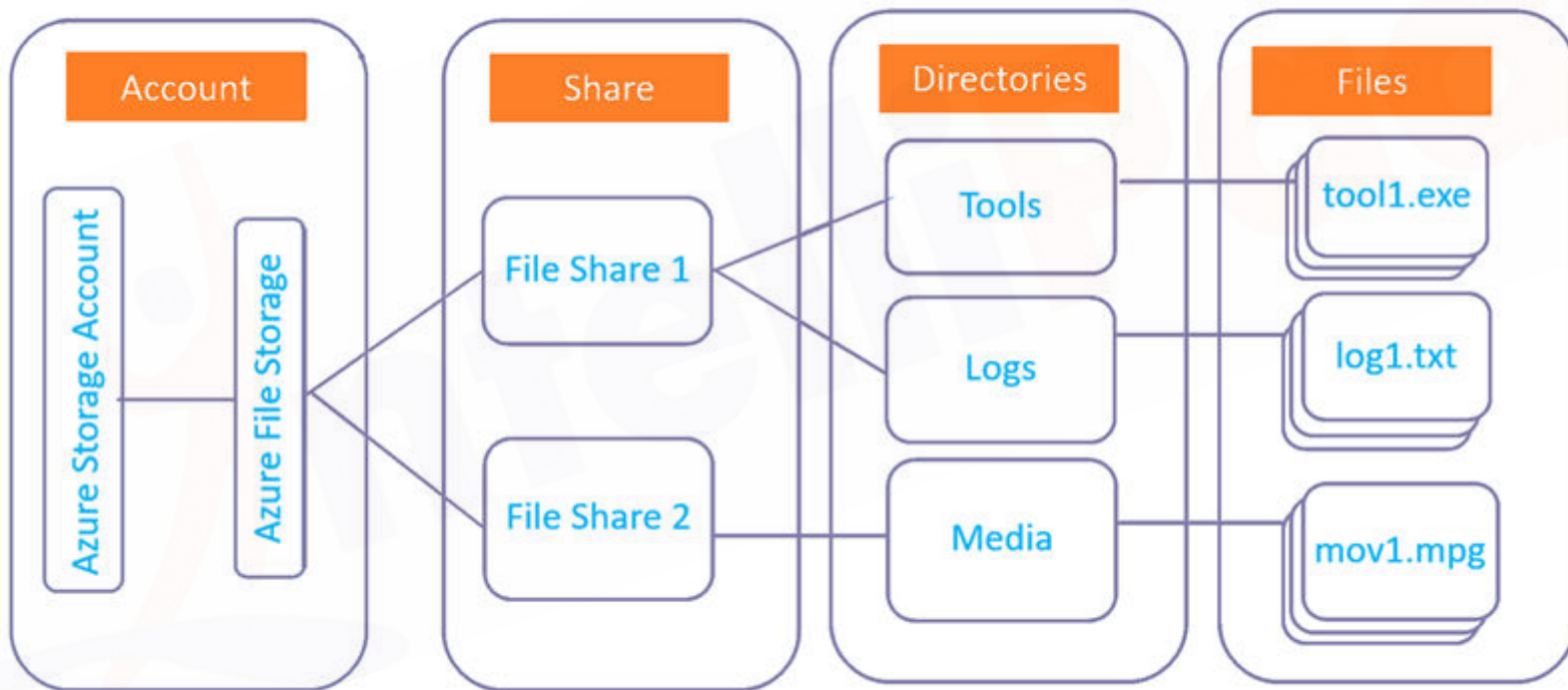# Use Cases

|	
Replace or supplement on-premises file servers	• Azure Files can be used to completely replace or supplement traditional on-premises file servers or NAS.
"Lift and shift" applications	• Azure Files make it easy to "lift and shift" applications to the cloud that expect a file share to store the file application or the user data.

Azure Files:
Constructs

Azure Files:
Management

❑ An account can contain an unlimited number of shares, and a share can store an unlimited number of files, up to the 5 TiB total capacity of the file share.

❑ A file in the share may be up to 1 TiB in size.

❑ **URL format**

▪ For requests to an Azure File share made with the File REST protocol, files are addressable using the following URL format:

https://<storage account>.file.core.windows.net/<share>/<directory>/directories>/<file>
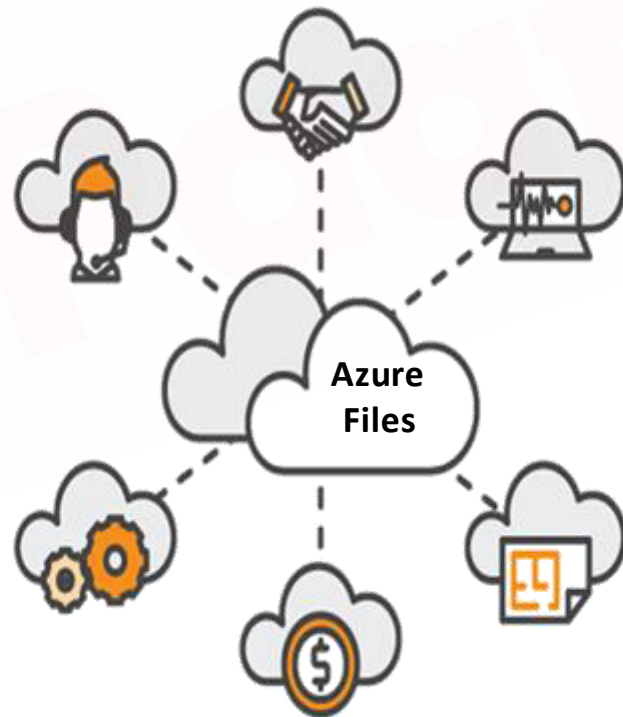
Azure Files

Azure Files:
Data Access Method

Azure Files offer two data access methods that you can use separately, or in combination with each other, to access your data:

- o **Direct Cloud Access**
  - ▪ Azure File share can be mounted by Windows, macOS, and/or Linux.
- o **Azure File Sync**
  - ▪ With Azure File Sync, shares can be replicated to Windows Servers on-premises or in Azure.
  - ▪ Users would access the file share through the Windows Server.
  - ▪ Data may be replicated between multiple Windows Server endpoints.
  - ▪ Data is tiered to Azure Files, but the Server does not have a full copy of the data.
  - ▪ Rather, data is seamlessly recalled when opened by your user.

Azure Table Storage

What Is Azure Table Storage?

❑ You can use the Azure Table storage service to store partially structured data in tables.

❑ Within each storage account, you can create multiple tables, and each table can contain multiple entities.

❑ Because table storage does not mandate a schema, the entities in a single table need not have the same set of properties.

Example:

    ❑ One product entity might have a size property, while another product entity in the same table might not have a size property at all.

    ❑ Each property consists of a name and a value.

❑ Similar to blobs, applications can access each table through a URL.

Example:

    ❑ To access a table named "**mytable**" in a storage account named "**myaccount**," applications would use the following link:

      http://myaccount.table.core.windows.net/mytable

Azure Table: Components
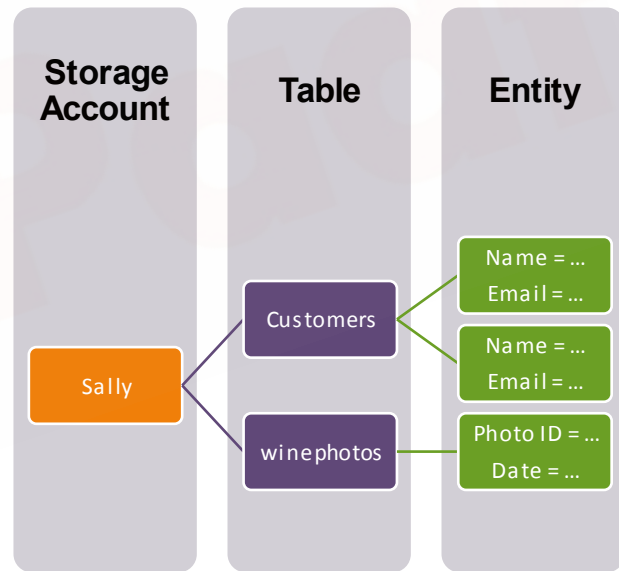
- ❑ **Storage Account**
- ❑ **Table**
  - ▪ A table is a collection of entities.
  - ▪ The number of tables that a storage account can contain is limited only by the storage account capacity limit.
- ❑ **Entity**
  - ▪ An entity is a set of properties, similar to a database row.
  - ▪ An entity can be up to 1 MB in size.
- ❑ **Properties**
  - ▪ A property is a name–value pair.
  - ▪ Each entity also has three system properties that specify a partition key, a row key, and a timestamp.

Storage Account	Table	Entity
Sally	Customers	Name = ... Email = ...
		Name = ... Email = ...
	winephotos	Photo ID = ... Date = ...

Azure Table: Service

❑ The Table service uses a tabular format to store data.

❑ In table, each row represents an entity and the columns

store various properties of that entity.

❑ Every entity also has three designated properties: a

partition key, a row key, and a timestamp.

❑ You can use the partition key to group similar entities based

on their common characteristics but with unique row key

values.

Azure Queue Storage

What Is Azure Queue Storage?

❑ The Azure Queue storage service provides a temporary messaging store.

❑ Developers frequently use queues to facilitate reliable exchange of messages between individual components of multitier or distributed systems.

❑ These components add and remove messages from a queue by issuing commands over the HTTP/HTTPS protocols.

❑ Similar to other Azure storage service types, in Azure Queue storage, each queue is accessible from a URL.

Example:

▪ To access a queue named "**myqueue**" in a storage account named "**myaccount**," applications would use:

http://myaccount.queue.core.windows.net/myqueue

❑ You can create any number of queues in a storage account and any number of messages in each queue up to the 500 TB limit for all data in the storage account.

❑ Each message can be up to 64 KB in size.

Azure Queue Storage: Components

❑ **URL format**

▪ Queues are addressable using the following URL format:

http://<storage account>.queue.core.windows.net/<queue>
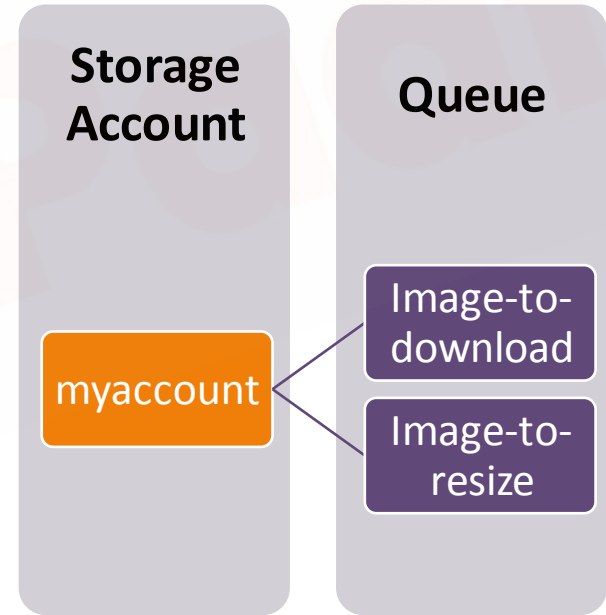
❑ **Storage account**

▪ All access to Azure Storage is done through a storage account.

❑ **Queue**

▪ A queue contains a set of messages.

▪ All messages must be in a queue.

❑ **Message**

▪ A message, in any format, of up to 64 KB.

▪ The maximum time that a message can remain in the queue is seven days.

Storage Account

Queue

myaccount

Image-to-download

Image-to-resize

Hands-on

Hands-on

- ❑ Create a storage account
- ❑ Create a blob and a container
- ❑ Upload and access data
- ❑ Configure security for data access

- ❑ Create a file share
- ❑ Connect and mount on the server and desktop

- ❑ Create a table storage
- ❑ Update and query the table

Virtual Network

What Is a Virtual Network?

❑ Azure networking components allow customers to create and manage virtual private networks in Azure.

❑ When you deploy computers in your on-premises environment, you typically connect them to a network to allow them to communicate directly with each other.

❑ Azure virtual networks (VNets) serve the same basic purpose. By placing a VM on the same VNet as other VMs, you effectively provide direct IP connectivity between them.

❑ You also have the option of connecting different VNets together.
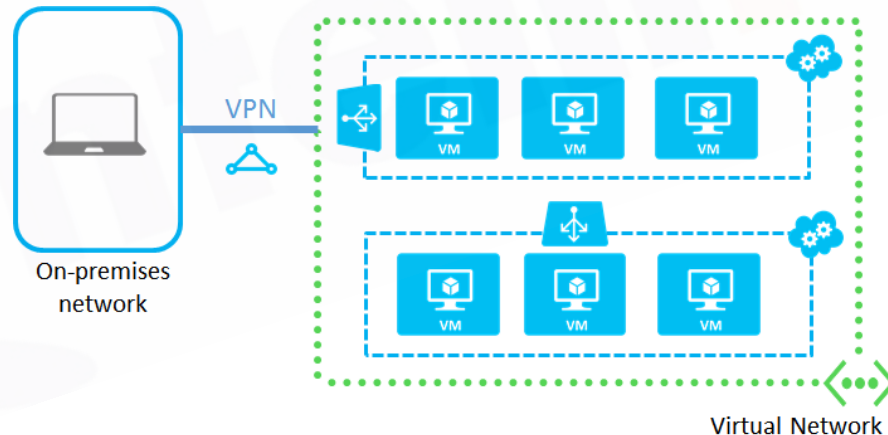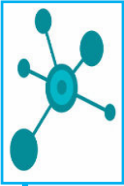
Azure Virtual Network: Features

Isolation

Internet Communication

Azure Resource Communication

Virtual Network Connectivity

On-premises Connectivity

Traffic Filtering

Routing

Azure Virtual Network

❑ An Azure VNet constitutes a logical boundary defined by a private IP address space.

❑ You divide this IP address space into one or more subnets.

❑ After you create a VNet, you cannot change its associated region.

❑ You must also specify the scope of the IP addresses that will be automatically assigned to the VMs that you deploy into that VNet.

❑ These IP address spaces are defined by RFC 1918 and include the following:

10.x.x.x	172.16.x.x – 172.31.x.x	192.168.x.x

❑ You should avoid overlapping address spaces across your Azure VNets and your on-premises networks.

❑ Overlapping address spaces will prevent you from connecting these networks later.

Azure Virtual Network: DHCP

❑ The Azure platform uses the Dynamic Host Configuration Protocol (DHCP) service to allocate IP addresses from the ranges you assign to VNet subnets.

❑ Each IP address lease has an infinite duration, but the lease is released if you *deallocate* (stop) the VM to which the IP address is assigned.

❑ To avoid IP address changes, configure a static private IP address.

Azure Virtual Network: Subnet

❑ Every VNet in Azure consists of one or more subnets.

❑ Subnets facilitate segmentation of networks.

❑ Subnets divide your VNet into smaller IP ranges so that the resources organized within these subnets can be logically separated.

❑ Each subnet contains a range of IP addresses that constitutes a subset of the VNet address space.

❑ The use of multiple subnets is common when implementing multi-tier applications, with one subnet per tier.

❑ If each tier resides on a separate subnet, you can assign a dedicated network security group to each subnet.

Virtual Networks

Subnet
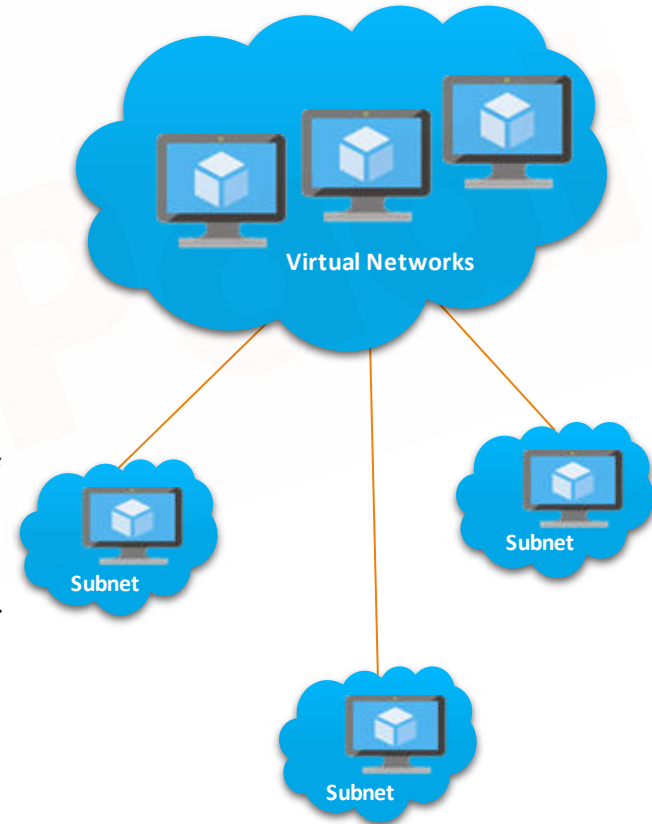
Subnet

Subnet

Azure Virtual Network: Routing

- Azure implements a default routing configuration to communicate with other resources.

- You can override some of Azure's system routes with custom routes.

- Azure routes outbound traffic from a subnet based on the routes in a subnet's route table.

System Routes
- Azure automatically creates system routes and assigns the routes to each subnet in a VNet.
- You can't create system routes nor can you remove system routes, but you can override them.
- Azure creates default system routes for each subnet.

Custom Routes
- Create custom routes by either creating user-defined routes.

Azure Virtual Network: Network Security Groups

❑ You can limit network traffic to resources in a VNet using a network security group.

❑ A network security group contains a list of security rules that allow or deny inbound or outbound network traffic.

❑ Each network interface or subnet can have zero or one associated network security group.

❑ When applied to a subnet, security rules are applied to all resources in the subnet.

Azure Virtual Network: NSG Rules
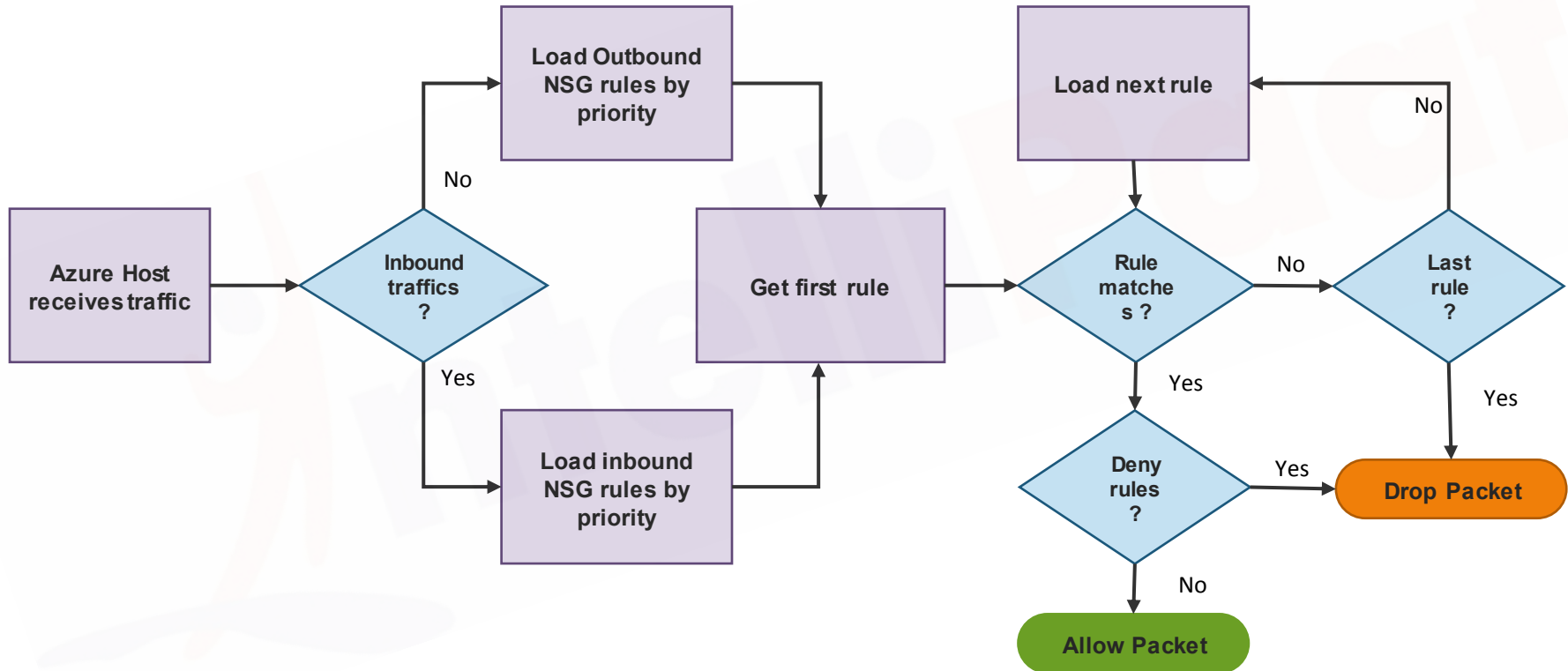
Azure Virtual Network: Service Endpoints

❏ VNet service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

❏ Endpoints allow you to secure your critical Azure service resources to only your virtual networks.

❏ Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.

❏ This feature is available in preview for the following Azure services and regions:
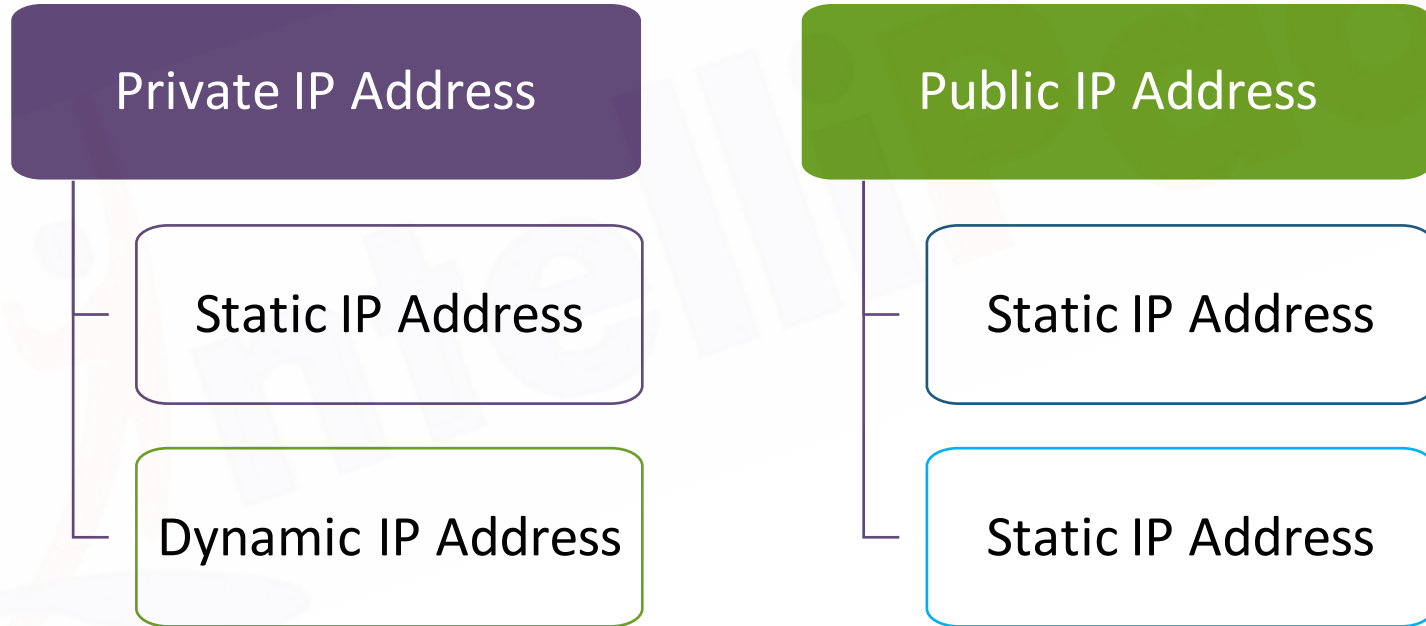
Azure Storage

All regions in the Azure public cloud.

Azure SQL

All regions in the Azure public cloud.

Azure Virtual Network: IP Address

Private IP Address

- Static IP Address
- Dynamic IP Address

Public IP Address

- Static IP Address
- Static IP Address

Azure Virtual Network: Connectivity Options
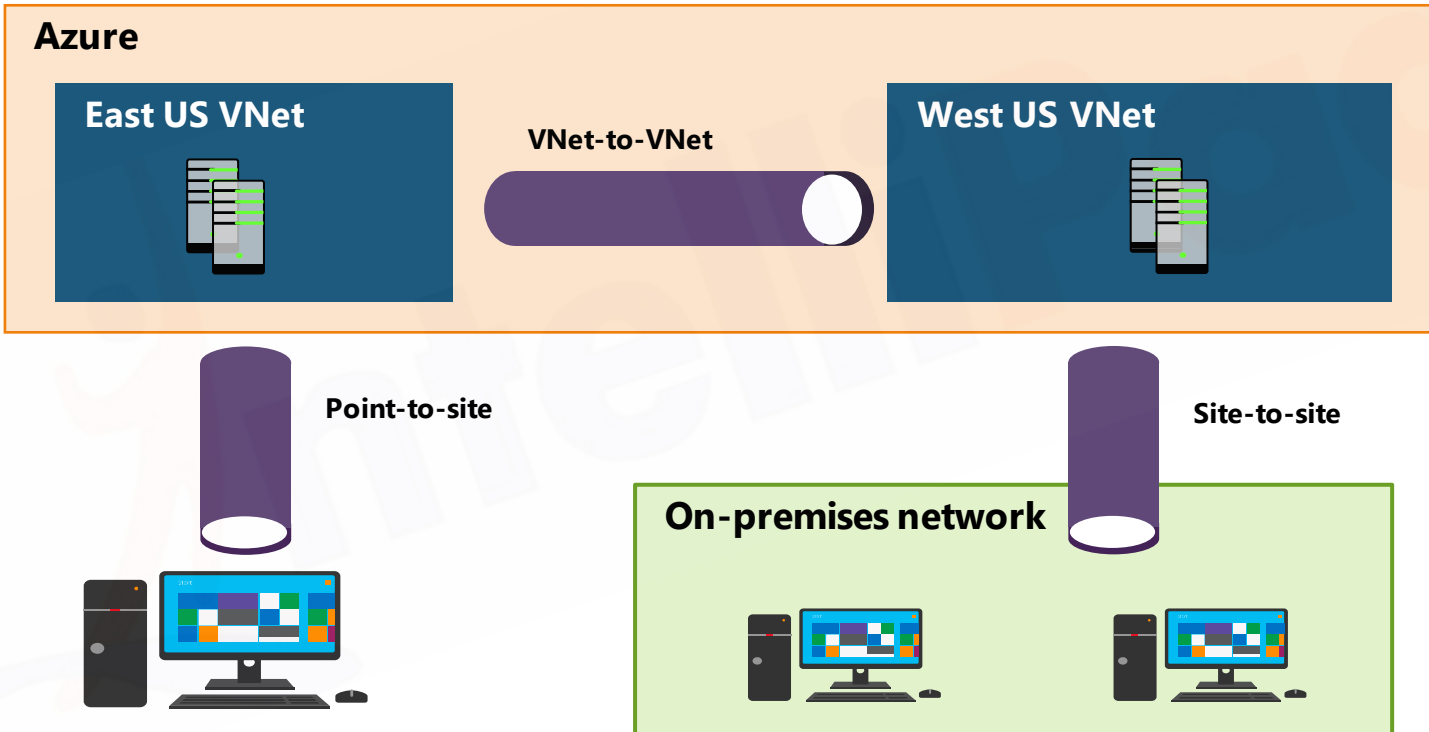
Azure Virtual Network: Connectivity Options

❑ Use connectivity options to allow VMs hosted on a VNet to communicate via private IP from computers that are not connected directly to the same VNet.

❑ If these computers reside outside Azure, you can use one of the following methods:

A point-to-site VPN	**A site-to-site VPN**	**Azure ExpressRoute**

❑ If these computers reside on another Azure VNet, you can use one of the following methods:

|	
VNet peering	**VNet-to-VNet connection**

Azure Virtual Network: VNet Peering

❑ VNet peering enables you to seamlessly connect two Azure VNets.

❑ VNet peering requires both VNets to reside in the same region.

❑ Once peered, the VNets appear as one, for connectivity purposes.

❑ Benefits of using VNet peering include:

VNet Peering

Network traffic between peered VNets is private.	Traffic between the VNets is kept on the Microsoft backbone network.	Resources in one VNet can communicate with resources in a different VNet, once the VNets are peered.
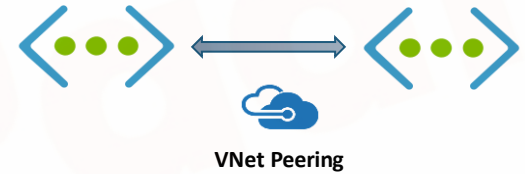
❑ VNet peering is nontransitive. This means that if you establish VNet peering between VNet1 and VNet2 and between VNet2 and VNet3, VNet peering capabilities do not apply between VNet1 and VNet3.

Hands-on

Hands-on

- ❑ Create a virtual network

- ❑ Create two subnets

- ❑ Launch the server in both subnets

- ❑ Install a web server

- ❑ Configure NSG at the subnet level

- ❑ Configure VNet peering

Azure DNS

What Is Azure DNS?

❑ The Domain Name System, or DNS, is responsible for translating (or resolving) a website or service name to its IP address.

❑ Azure DNS is a hosting service for DNS domains, providing name resolution using Microsoft Azure infrastructure.

❑ By hosting your domains in Azure, you can manage your DNS.

❑ Azure DNS also supports private DNS domains.

User

1.) Request: www.contoso.com ▶

2.) Return IP: 1,2,3,4

Azure DNS

VM

Web App

3.) Connect to Resource with IP:1,2,3,4
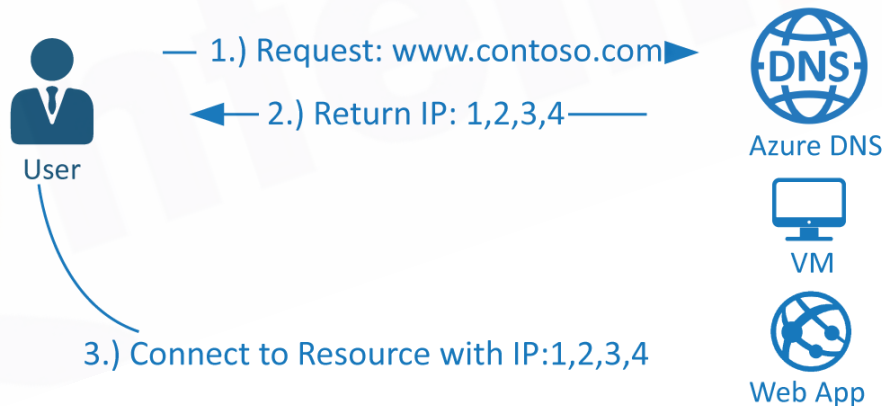
Azure DNS: Features

Reliability and Performance

- DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers.
- Azure DNS uses any cast networking so that each DNS query is answered by the closest available DNS server.
- This provides both fast performance and high availability for your domain.

Seamless Integration

- The Azure DNS service can be used to manage DNS records for your Azure services and can be used to provide DNS for your external resources as well.

Security

- The Azure DNS service is based on Azure Resource Manager.
- Your domains and records can be managed via the Azure portal, Azure PowerShell cmdlets, and the cross-platform Azure CLI.

Azure DNS: Domain

❑ The Domain Name System is a hierarchy of domains.

❑ The hierarchy starts from the 'root' domain, whose name is simply '**.**'.

  ▪ Top-level domains include 'com,' 'net,' 'org,' 'uk,' or 'jp.'

  ▪ Then, there are second-level domains, such as 'org.uk' or 'co.jp.'

❑ The domains in the DNS hierarchy are globally distributed, hosted by DNS name servers around the world.

❑ A domain name registrar is an organization that allows you to purchase a domain name, such as 'contoso.com.'

❑ Azure DNS provides a globally distributed, high-availability name server infrastructure, which you can use to host your domain.

❑ By hosting your domains in Azure DNS, you can manage your DNS record.

❑ Azure DNS does not currently support purchasing of domain names. If you want to purchase domains, you need to use a third-party domain name registrar.

Azure DNS: DNS Zones

❏ A DNS zone is used to host the DNS records for a particular domain.

❏ To start hosting your domain in Azure DNS, you need to create a DNS zone for that domain name.

❏ Each DNS record for your domain is then created inside this DNS zone.

Example
The domain 'contoso.com' may contain several DNS records, such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site).

❏ When creating a DNS zone in Azure DNS:

The name of the zone must be unique within the resource group, and the zone must not exist already.	The same zone name can be reused in a different resource group or a different Azure subscription.	Where multiple zones share the same name, each instance is assigned different name server addresses.	Only one set of addresses can be configured with the domain name registrar.

Azure DNS: DNS Records

Record Names

In Azure DNS, records are specified by using relative names. A *fully qualified* domain name (FQDN) includes the zone name, whereas a *relative* name does not.

For example, the relative record name 'www' in the zone 'contoso.com' gives the fully qualified record name 'www.contoso.com.'

Record Types

Each DNS record has a name and a type.

Records are organized into various types according to the data they contain.

The most common type is an 'A' record, which maps a name to an IPv4 address.

Another common type is an 'MX' record, which maps a name to a mail server.

Azure DNS supports all common DNS record types: A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV, and TXT.
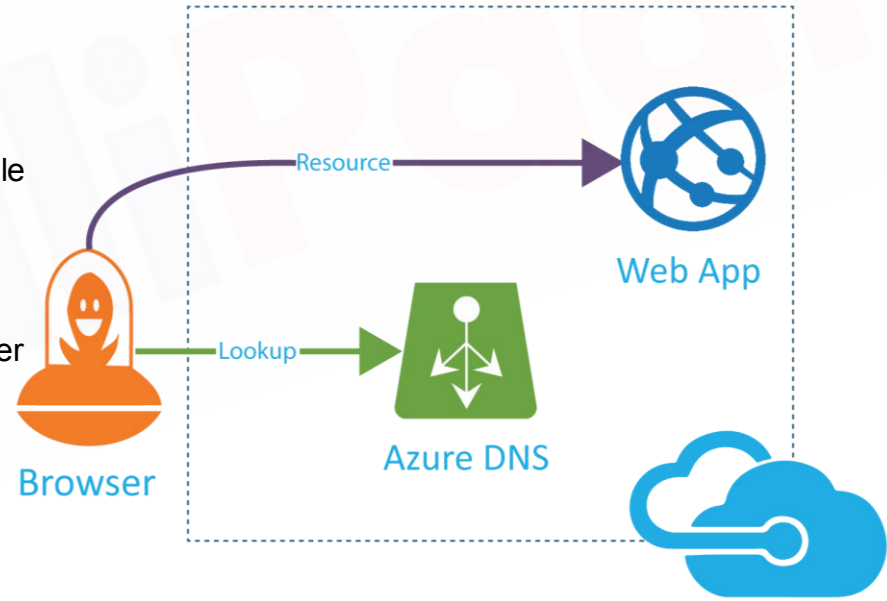
Azure DNS:

DNS Record

Record Type	Full Name	Function
A (IPv4) AAAA (IPv6)	Address	Maps a host name such as 'www.adatum.com' to an IP address, such as '131.107.10.10'
CNAME	Canonical Name	Assigns a custom name, such as 'ftp.adatum.com,' to a host record, such as 'host1.adatum.com'
MX	Mail Exchange	Points to the host that accepts email for the domain. MX records must point to an A record and not to a CNAME record
NS	Name Server	Contains the name of a server hosting a copy of the DNS zone
SOA	Start of Authority	Provides information about the writable copy of the DNS zone, including its location and version number
SRV	Service	Points to hosts that are providing specific services, such as the Session Initiation Protocol (SIP) or Active Directory Domain Services (AD DS)
TXT	Text	Contains custom text

# Azure DNS: Registrar

❑ A domain registrar is a company who can provide Internet domain names.

❑ They verify if the Internet domain you want to use is available and allow you to purchase it.

❑ Once the domain name is registered, you are the legal owner for the domain name.

❑ If you already have an Internet domain, you will use the current domain registrar to delegate to Azure DNS.

Azure DNS:
Private Domains

❑ Azure DNS is a hosting service for DNS domains.

❑ In addition to Internet-facing DNS domains, Azure DNS now also supports private DNS domains.

❑ Azure DNS resolves domain names in a VNet without the need to add a custom DNS solution.

❑ Private DNS zones allow you to use your own custom domain names rather than the Azure-provided names.

❑ It provides name resolution for VMs within a VNet and between VNets.

❑ Additionally, you can configure zones names with a split-horizon view, allowing a private and a public DNS zones to share the same name.
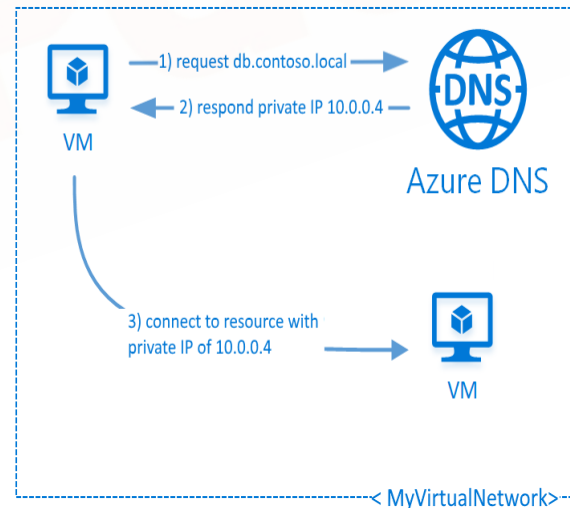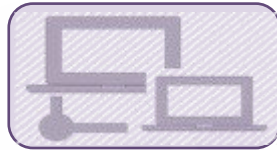
Azure DNS:

Private Domains' Benefits

Remove the need for custom DNS solutions

- DNS zone management can now be done using Azure's native infrastructure, which removes the burden of creating and managing custom DNS solutions.

Automatic hostname record management

- Along with hosting your custom DNS records, Azure automatically maintains hostname records for the VMs in specified VNets.
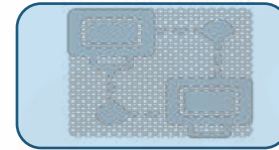
Hostname resolution between VNets

- Unlike Azure-provided hostnames, private DNS zones can be shared between VNets. This capability simplifies cross-network and service discovery scenarios such as VNet peering.

Split-horizon DNS support

- Azure DNS allows you to create zones with the same name that resolve to different answers from within a VNet and from the public Internet.

Familiar tools and user experience

Use all common DNS record types

Hands-on

Hands-on

- ☐ Register a DNS name

- ☐ Create a DNS zone

- ☐ Update the name server

- ☐ Create a resource record

- ☐ Access the web server using the DNS name

What Is Azure AD?

What Is Azure AD?

❑ Azure Active Directory (Azure AD) is a cloud-based directory and identity management.

❑ By using Azure AD, you can provide secure access to sensitive services and data and single sign-on (SSO).

❑ Azure AD supports:

Multi-factor authentication for both on-premises and cloud-resident resources.	Role-based Access Control (RBAC)	Self-service password	Group management	Device registration

❑ Organizations that use AD DS can synchronize users and groups from their Active Directory domains with Azure AD to enable an SSO experience for their users accessing both on-premises and cloud-based applications.

Azure AD:

Azure AD Editions

Free Edition

- Provides user and group management, device registration, self-service password change for cloud users, and synchronization with on-premises directories.
- It is limited to 10 applications per user configured for SSO and 500,000 objects.

Basic Edition

- Extends the free edition's capabilities by combining group-based access management, self-service password reset for cloud users, and support for application proxy.
- It does not impose limits on the number of directory objects, but it has a limit of 10 apps per user.

Premium Edition

- It supports dynamic group and self-service group management and self-service password reset.
- It offers support for an unlimited number of objects and unlimited number of apps per user.
- Azure AD Premium is available in two tiers: P1 and P2. Both tiers include all features described above.
- Azure AD Premium P2, however, offers additional identity protection and privileged identity management features.

Azure AD:
AD Domain Services

❑ Active Directory Domain Services (AD DS) is a directory service and an identity management solution.

❑ As a directory service, AD DS hosts a distributed database residing on servers referred to as domain controllers.

❑ When comparing AD DS with Azure AD, it is important to note the following characteristics of AD DS:
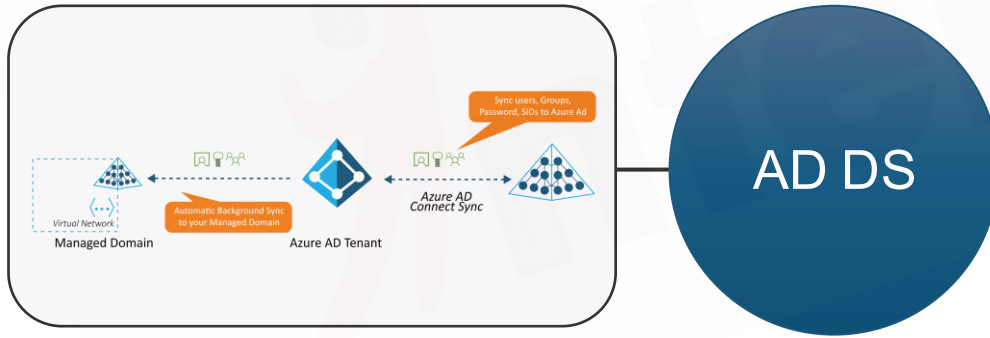
AD DS

- ❑ AD DS is by design single tenant.
- ❑ AD DS uses DNS for locating domain controllers.
- ❑ AD DS relies on protocols such as Lightweight Directory Access Protocol (LDAP) for directory lookups and Kerberos for authentication.
- ❑ AD DS facilitate Group Policy Objects (GPOs)–based management.
- ❑ AD DS supports users, groups, and AD-aware applications.
- ❑ AD DS supports computer objects, representing computers that join an Active Directory domain.
- ❑ AD DS supports multi-domain forests.

Azure AD: Overview

❑ Azure AD is somewhat similar to AD DS; however, there are some fundamental differences between them.

❑ The following are some of the characteristics that make Azure AD distinct:

01 Azure AD is multitenant by design.

02 Azure AD provides no support for organizational units (OUs).

03 Azure AD implementation does not rely on domain controllers.

04 Azure AD supports protocols that facilitate secure communication over the Internet.

05 Azure AD does not support kerberos authentication; instead, it uses protocols such as saml, ws-federation, and openID connect for authentication (and OAuth for authorization).

06 Azure AD does not support LDAP; instead, it relies on graph application programming interface (API) for directory lookups.

07 Azure AD provides no support for GPOs.

08 AD DS supports users, groups, and web-based applications.

09 Azure AD supports device objects representing devices that register or join an Azure AD tenant.

10 Azure AD offers federation services, and many third-party services (such as Facebook) are federated with and trust Azure AD. You can also federate AD DS with Azure AD.

Azure AD:
Custom Domain Names

AZURE ACTIVE DIRECTORY
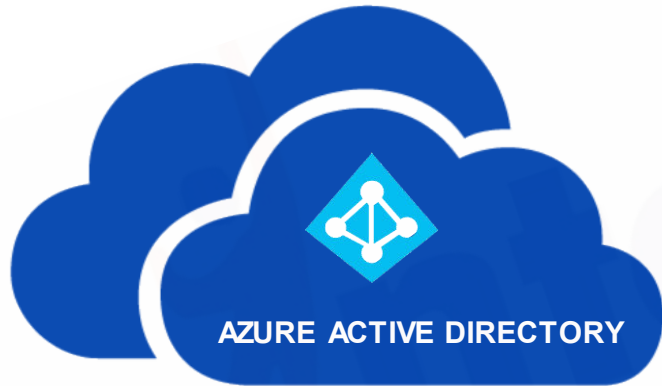
01 Each Azure AD tenant is assigned the default DNS domain name, consisting of a unique prefix, followed by the onmicrosoft.com suffix.

02 The prefix is either derived from the name of the Microsoft account you use to create an Azure subscription or provided explicitly when you create an Azure AD tenant.

03 It is common to add at least one custom domain name to the same Azure AD tenant.

04 This name utilizes the DNS domain namespace that the tenant's company or organization owns.

Azure AD:
Managing Users, Groups, and Devices

❑ You can manage Azure AD users, groups, and devices by using the Azure portal, Active Directory PowerShell, Microsoft Intune admin console, or Office 365 admin center.

❑ There are three basic ways to create users, groups, and devices in Azure AD:

As cloud identities defined directly in the Azure AD tenant.

As directory-synchronized identities generated through synchronization between on-premises Active Directory and an Azure AD tenant.

You also have the option of creating guest users, which represent users defined in other Azure AD tenants or other federated identity providers.
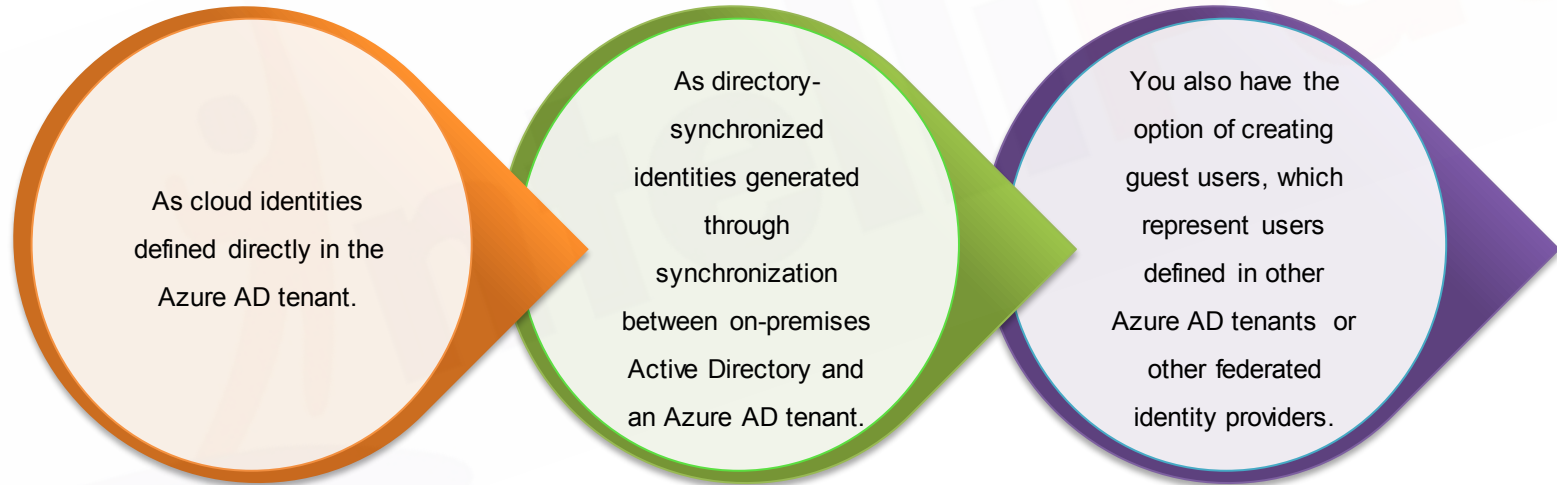
Azure AD:

Managing Devices

Users can join their Windows 10 devices to Azure AD.

If users use their Azure AD credentials to sign in to Windows 10, they can benefit from SSO functionality when accessing Office 365 and any other applications that use Azure AD for authentication, including the Azure AD Access Panel.

You can disable the ability to join devices to Azure AD or restrict it to specific Azure AD users or groups.

You can also limit the maximum number of devices per user and enforce multi-factor authentication when joining devices in Azure AD.

After a user registers a device in Azure AD, you can control its usage.

For example, if you determine that the device has been lost or compromised, you can delete its Azure AD object or block its ability to authenticate.

Azure AD: Tenants

❑ By default, you automatically get an Azure AD tenant when you sign up for an Azure, Office 365, Microsoft Dynamics CRM Online, or Microsoft Intune subscription.

❑ That tenant authenticates users defined in its directory.

❑ You can also create additional tenants as needed.

❑ Support for multiple Azure AD tenants facilitates the following scenarios:

Creating separate directories for testing or other non-production purposes.	Managing multiple Azure AD tenants by using the same user credentials—as long as the corresponding user account is a Global administrator in each of them.	Adding existing users as guests to multiple Azure AD tenants and eliminating the need to maintain multiple credentials for the same user.

Azure AD: SSO

To avoid additional authentication prompts when launching applications, configure SSO.

SSO allows users to run Azure AD–registered applications without providing a user name and password.

SSO eliminates the need to provision and maintain separate user accounts for each SaaS application.

Azure AD provides secure storage of user credentials and provides support for federated trusts with other cloud services and identity providers.

Several commercial applications with SSO capabilities, such as Microsoft Office 365, Box, or Salesforce, are preconfigured for integration with Azure AD.

You can also use Azure AD SSO functionality to control access to on-premises applications or applications developed in-house but deployed to Azure.

Hands-on

Hands-on

- ❑ Configure Azure AD

- ❑ Create a user in Azure AD

- ❑ Login via Azure AD

- ❑ Enable MFA

QUIZ

Quiz 1

Which one of them is the Object based storage in Azure?

A	Azure Queue Storage
B	Azure Data lake storage
C	Azure Storage explorer
D	Azure Blob storage

Answer 1

Which one of them is the Object based storage in Azure?

A	Azure Queue Storage
B	Azure Data lake storage
C	Azure Storage explorer
D	Azure Blob storage

Quiz 2

Limitless storage for data analytics?

A   Azure Archive Storage

B   Azure Blob storage

C   Azure Data lake storage

D   Azure Storage explorer

Answer 2

Limitless storage for data analytics?

A	Azure Archive Storage
B	Azure Blob storage
C	Azure Data lake storage
D	Azure Storage explorer

Quiz 3

What does azure uses to allocate IP addresses?

A	Dynamic Host Configuration Protocol
B	Domain Name System
C	Network Security Group
D	Vnet Peering

Answer 3

What does azure uses to allocate IP addresses?

| A | Dynamic Host Configuration Protocol |

| B | Domain Name System |

| C | Network Security Group |

| D | Vnet Peering |

Quiz 4

Which statement is true about Routing in Virtual Network?

A You can configure and manage your VM connections using routing.

B You can configure and manage your VM connections using routing.

C You can create a custom VM using routing.

D You can communicate with other resources using routing.

Answer 4

Which statement is true about Routing in Virtual Network?

A You can configure and manage your VM connections using routing.

B You can configure and manage your VM connections using routing.

C You can create a custom VM using routing.

D You can communicate with other resources using routing.

Quiz 5

Once applied to a subnet, can you apply the security rules to all the resources in the subnet?

A Yes

B No

Answer 5

Once applied to a subnet, can you apply the security rules to all the resources in the subnet?

A Yes

B No

Quiz 6

Network traffic between virtual networks is_____?

A	Private
B	Public
C	Hybrid
D	**Closed**

Answer 6

Network traffic between virtual networks is_____?

A	Private
B	Public
C	Hybrid
D	**Closed**

Quiz 7

Using Vnet peering, you can connect
_____?

A	Any 2 Azure Virtual Networks
B	Any 4 Azure Virtual Networks
C	Any 6 Azure Virtual Networks
D	Any amount of Virtual Networks

Answer 7

Using Vnet peering, you can connect _____?

A	Any 2 Azure Virtual Networks
B	Any 4 Azure Virtual Networks
C	Any 6 Azure Virtual Networks
D	Any amount of Virtual Networks

Quiz 8

Vnet Peering is   ?

A	Transitive
B	Non-transitive
C	Open
D	Private

Answer 8

Vnet Peering
is   ?

A Transitive

B Non-transitive

C Open

D Private

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

sales@intellipaat.com

24/7 Chat with Our Course Advisor