Microsoft Azure

Administrator Associate Training

Configure & Manage Virtual Networks

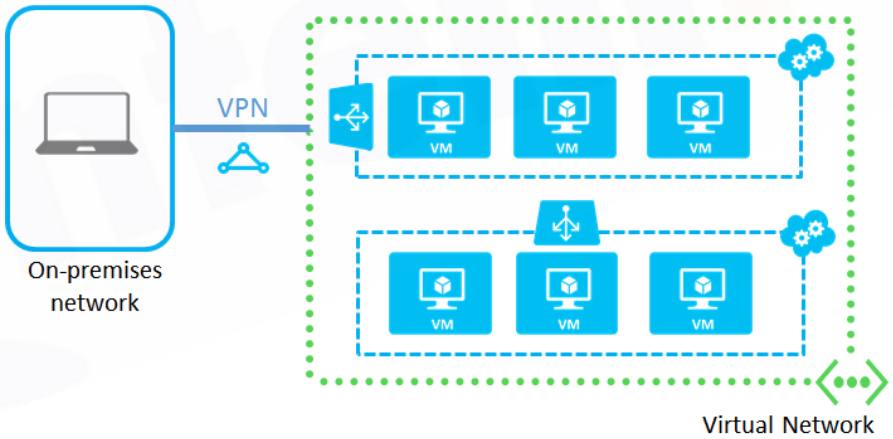
Agenda

- What is Virtual Network?
- Azure VNet Features
- Azure Virtual Network
- DHCP
- Subnet
- Routing
- Network Security Groups
- NSG Rule
- Service Endpoints
- IP Address
- Connectivity Options
- VNet Peering
- What is Azure DNS?
- Azure DNS features
- Domain
- DNS zones
- DNS records
- DNS records types
- Registrar
- Private domains
- Private domains benefits
- Pricing

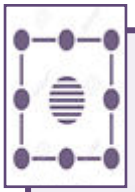
Virtual Network

What is Virtual Network?

- Azure networking components allow customers 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 serve the same basic purpose. By placing a virtual machine on the same virtual network as other virtual machines, you effectively provide direct IP connectivity between them.
- You also have the option of connecting different virtual networks together.

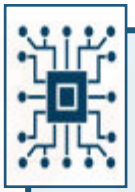


Azure Virtual Network: Features

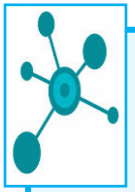


Isolation

Internet Communication



Azure Resource Communication



Virtual Network Connectivity

On-premises Connectivity

Traffic Filtering

Routing

Azure Virtual Network:
Virtual Network

- An Azure virtual network 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 virtual network, you cannot change its associated region.
- you must also specify the scope of the IP addresses that will be automatically assigned to virtual machines that you deploy into that virtual network.
- 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

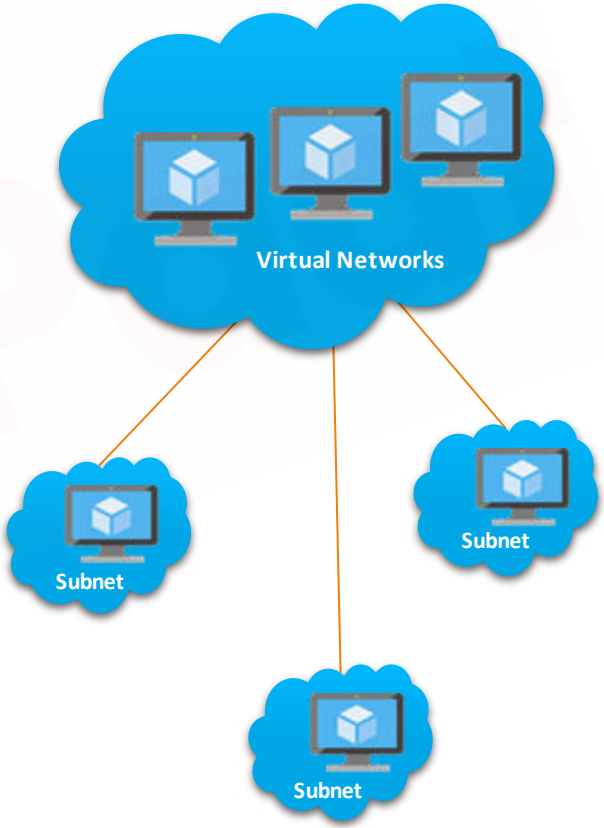
- You should avoid overlapping address spaces across your Azure virtual networks and your on-premises networks.
- Overlapping address spaces will prevent you from connecting these networks later.

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 virtual network subnets.
- Each IP address lease has an infinite duration, but the lease is released if you *deallocate (stop)* the virtual machine to which the IP address is assigned.
- To avoid IP address changes, configure a static private IP address.

Azure Virtual Network: Subnet

- Every virtual network in Azure consists of one or more subnets.
- Subnets facilitate segmentation of networks.
- Subnets divide your virtual network 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 constitute a subset of the virtual network 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.



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 virtual network.
- You can't create system routes, nor can you remove system routes, but you can override system routes.
- Azure creates default system routes for each subnet.

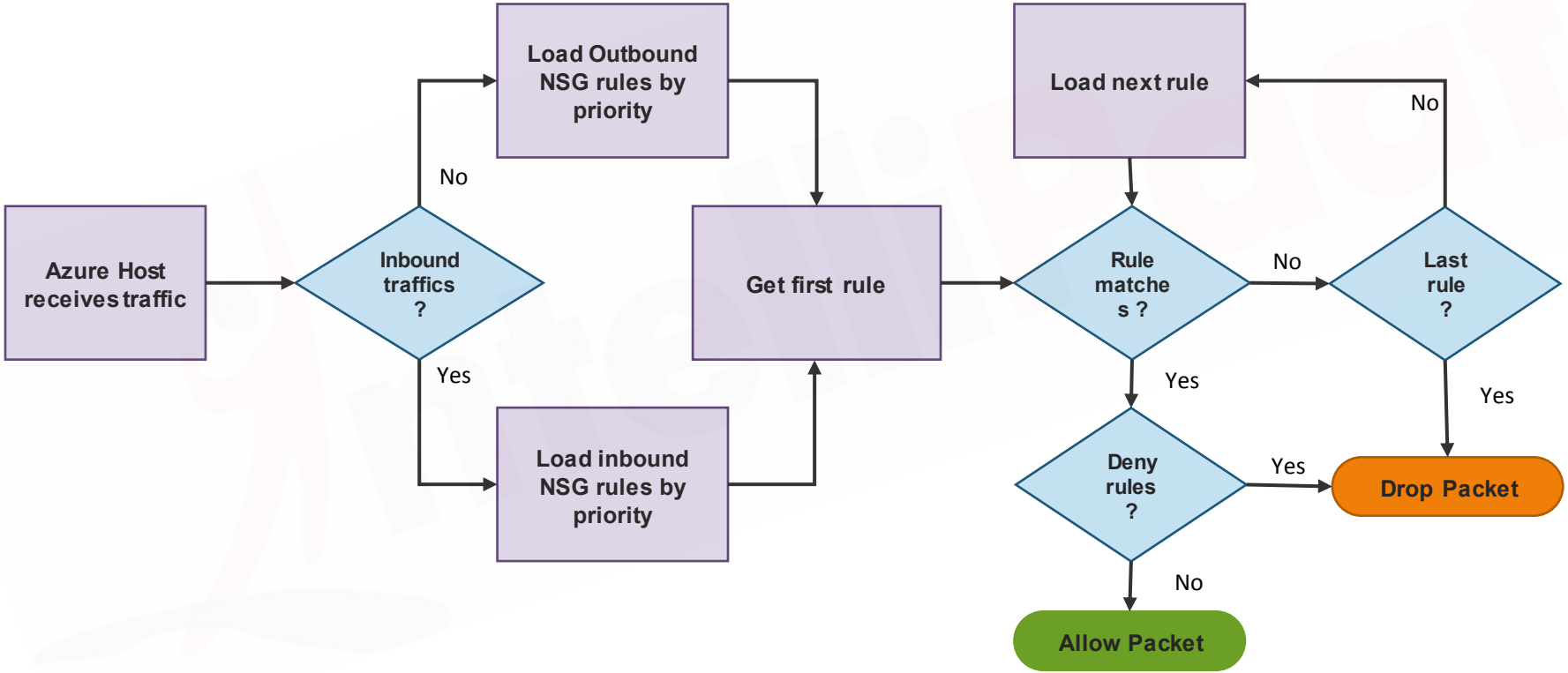
Custom Routes

- You 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.

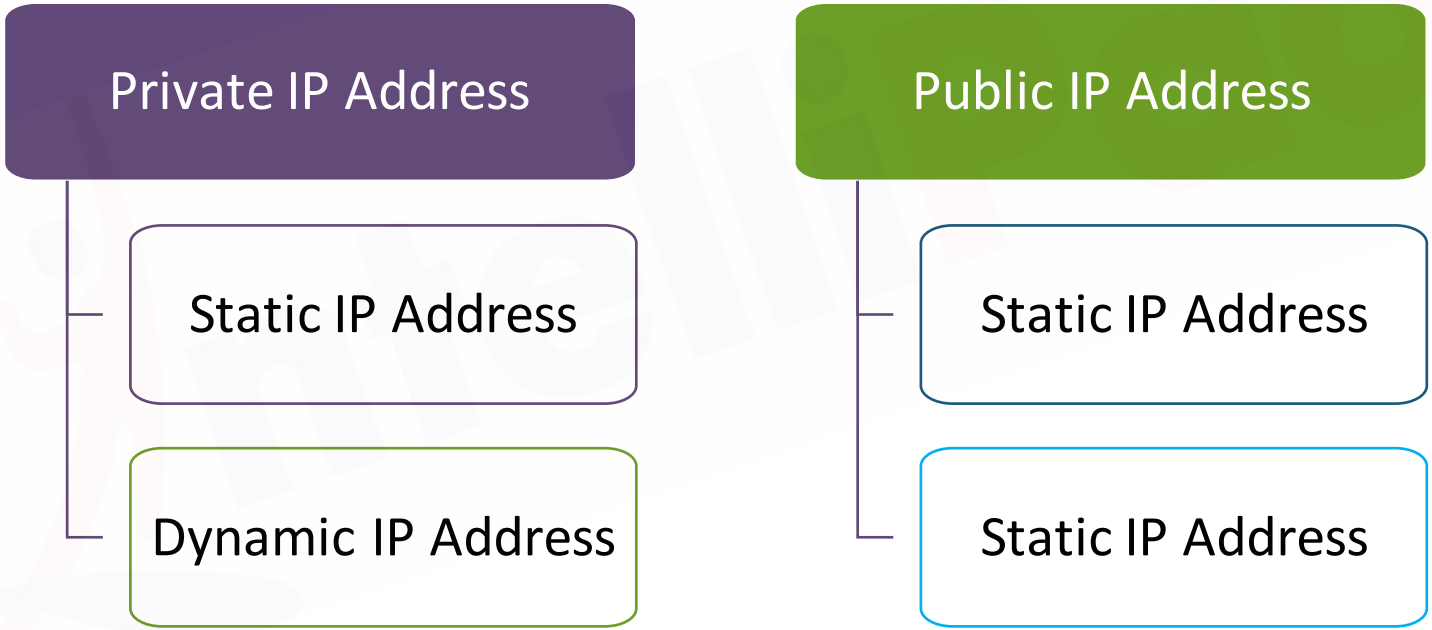
Azure Virtual Network:
NSG Rule



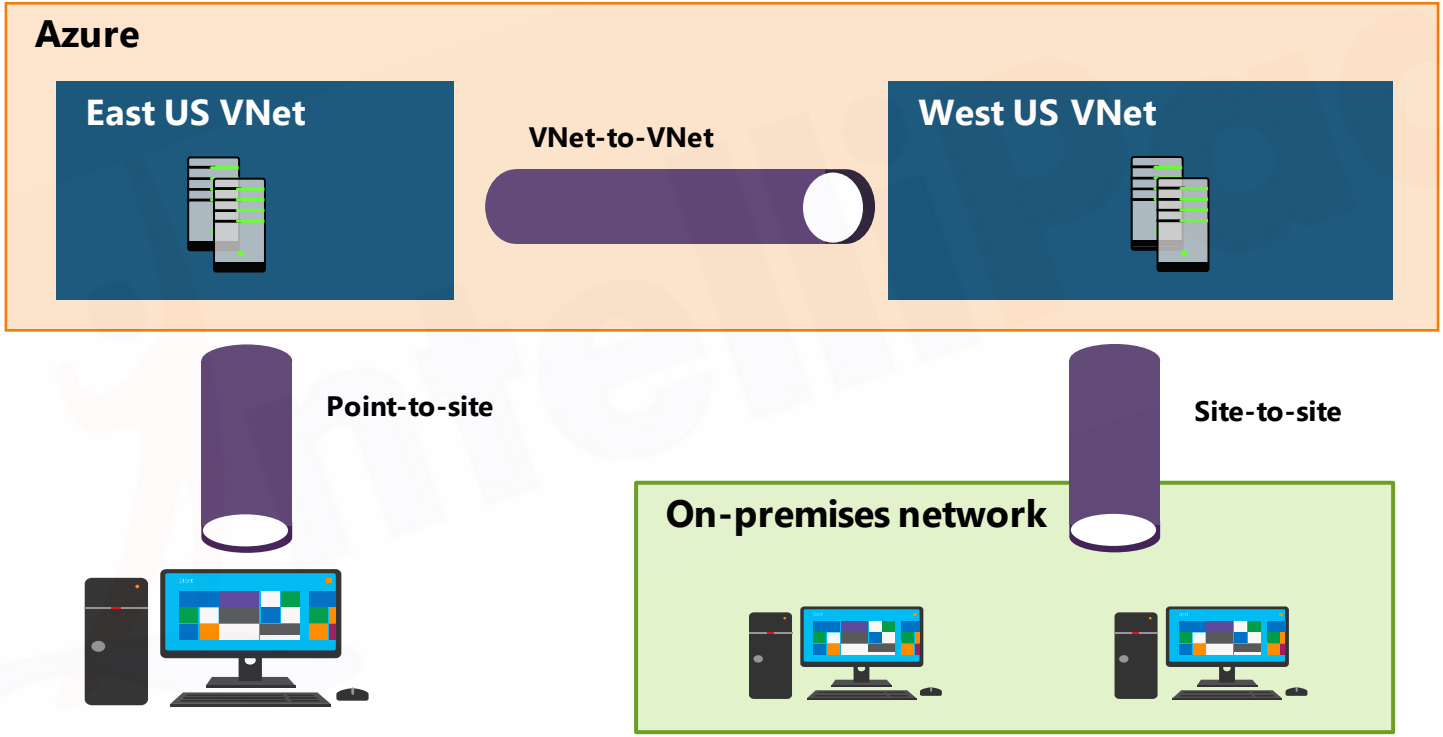
Azure Virtual Network: Service Endpoints

- 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 Virtual Network:
IP Address



Azure Virtual Network: Connectivity Options



Azure Virtual Network: Connectivity Options

- Use Connectivity options to allow VMs hosted on an 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 virtual network, 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 virtual networks.
- VNet peering required both virtual networks reside in the same region.
- Once peered, the virtual networks appear as one, for connectivity purposes.
- The benefits of using virtual network peering include:

Network traffic between peered virtual networks is private.

Traffic between the virtual networks is kept on the Microsoft backbone network.

The ability for resources in one virtual network to communicate with resources in a different virtual network, once the virtual networks 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

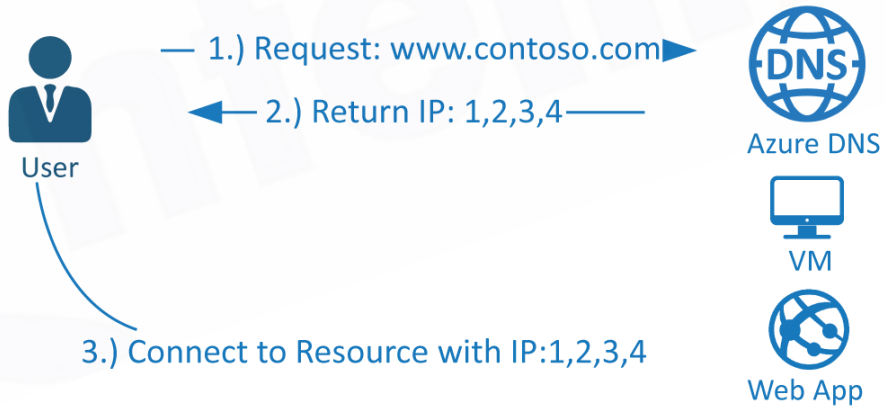
Hands-On

- Create virtual network
- Create 2 subnet
- Launch server in both subnet
- Install web server
- Configure NSG at 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.



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 anycast 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, such as 'com', 'net', 'org', 'uk' or 'jp'.
  - Then 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

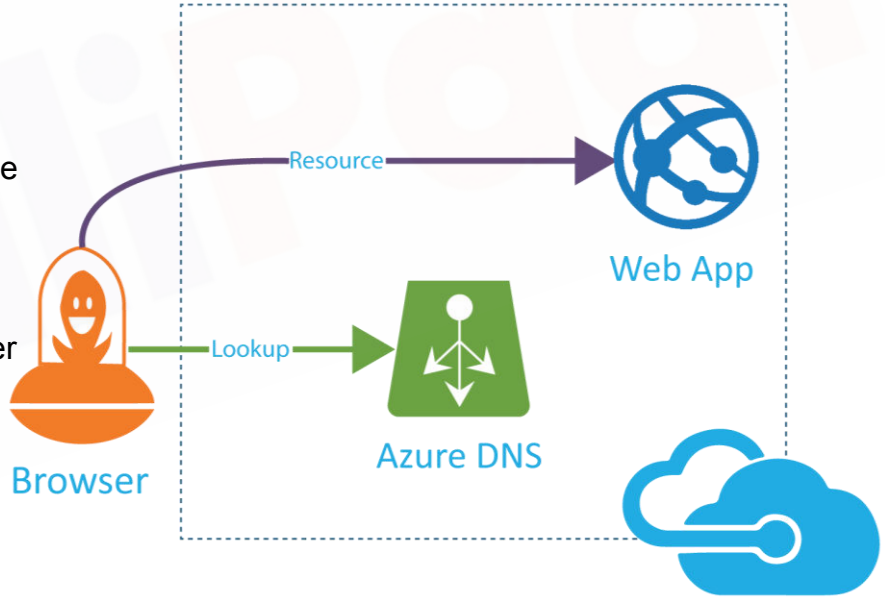
Azure DNS:

DNS Records

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.

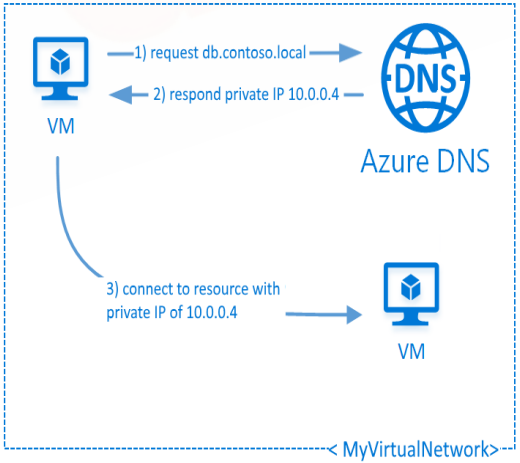
Azure DNS: Registrar

- 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 resolve domain names in a virtual network 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 virtual network and between virtual networks.
- Additionally, you can configure zones names with a split-horizon view - allowing a private and a public DNS zone to share the same name.

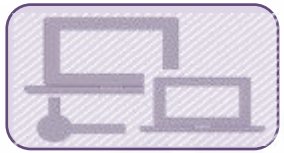


Azure DNS:

Private Domains Benefits

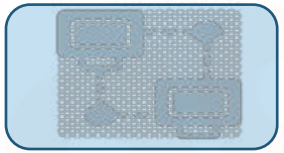
Removes the need for custom DNS solutions

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



Automatic hostname record management

- Along with hosting your custom DNS records, Azure automatically maintains hostname records for the VMs in the specified virtual networks.



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.

Split-horizon DNS support

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

Familiar tools and user experience

Use all common DNS records types

Hands-On

Hands-On

- Register DNS name
- Create DNS zone
- Update name server
- Create resource record
- Access web server using DNS name

QUIZ

Quiz 1

Azure Virtual Network_____?

A	Lets you create and manage your local networks
B	Lets you create and manage your virtual machines
C	Lets you create and manage your local networks in your virtual machines
D	Lets you create and manage virtual private networks in Azure Cloud.

Answer 1

Azure Virtual Network_____?

A	Lets you create and manage your local networks
B	Lets you create and manage your virtual machines
C	Lets you create and manage your local networks in your virtual machines
D	Lets you create and manage virtual private networks in Azure Cloud.

Quiz 2

Can you change the associated region of a virtual network after its creation?

A	Yes
B	No

Answer 2

Can you change the associated region of a virtual network after its creation?

A	Yes
B	No

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

24X7 Chat with our Course Advisor