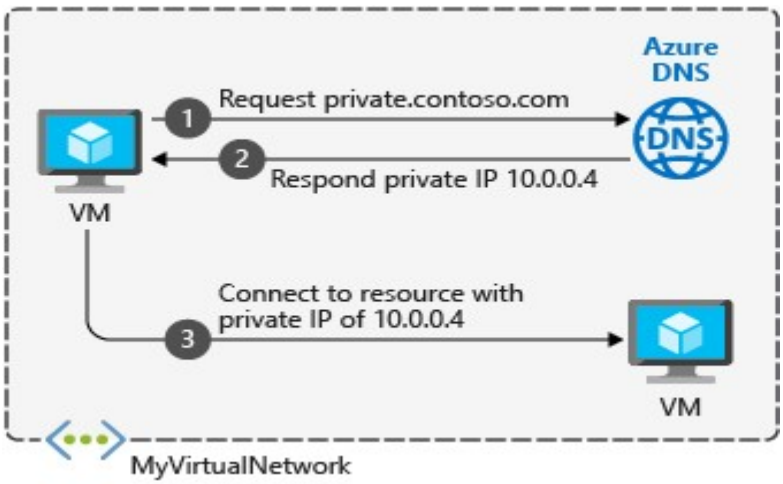
What is Azure private DNS ?

An Azure Private DNS zone is a managed DNS service that provides name resolution for private resources in Azure.

Private DNS zones are hosted in Azure, but they are not accessible from the public internet. Instead, they are only accessible to resources within virtual networks that are linked to the zone.

Private DNS zones can be used to resolve the names of a variety of Azure resources, including:

- Virtual machines
- Cloud services
- Azure App Service
- Azure Kubernetes Service
- Azure Container Instances
- Azure Database for PostgreSQL
- Azure Database for MySQL



Private DNS zones also support custom DNS records, such as A records, CNAME records, and MX records. This allows you to use your own custom domain names for your Azure resources.

There are several benefits to using Azure Private DNS zones, including:

- **Security**: Private DNS zones help to protect your resources from unauthorized access. Because private DNS zones are not accessible from the public internet, only resources within linked virtual networks can resolve the names of resources in the zone.

- **Reliability**: Azure Private DNS zones are highly reliable and scalable. They are backed by the same global infrastructure that powers Azure DNS.

- **Flexibility**: Private DNS zones can be used to resolve the names of a variety of Azure resources, including virtual machines, cloud services, and Azure App Service. They also support custom DNS records, so you can use your own custom domain names for your Azure resources.

How to use Azure Private DNS ?

To use an Azure Private DNS zone, We first need to create the zone. Once the zone is created, you can link it to one or more virtual networks. You can also add DNS records to the zone. Once the zone is linked to a virtual network, resources in the virtual network will be able to resolve the names of resources in the zone.

Azure Private DNS zones are a powerful tool that can be used to improve the security, reliability, and flexibility of your DNS infrastructure in Azure.

only accessible to resources within virtual networks that are linked to the zone.

The records contained in a private DNS zone aren't resolvable from the Internet. DNS resolution against a private DNS zone works only from virtual networks that are linked to it.

You can link a private DNS zone to one or more virtual networks by creating virtual network links. You can also enable the autoregistration feature to automatically manage the life cycle of the DNS records for the virtual machines that get deployed in a virtual network.

- **Implement hybrid DNS**: Private DNS zones can be used to implement hybrid DNS, which allows you to resolve the names of on-premises resources from Azure and vice versa. This can be useful for organizations that are migrating workloads to Azure or that have a mix of on-premises and Azure resources.
- **Improve application performance**: Private DNS zones can be used to improve the performance of applications that rely on DNS lookups. By resolving DNS names within a virtual network, you can reduce the latency of DNS lookups and improve the overall performance of your applications.
- **Simplify application deployment:** Private DNS zones can be used to simplify the deployment of applications by eliminating the need to manually configure DNS records for each application. You can use Private DNS zones to create DNS records that are automatically updated when applications are deployed.

Capabilities

Azure Private DNS provides the following capabilities:

- **Automatic registration of virtual machines from a virtual network that's linked to a private zone with autoregistration enabled**. Virtual machines get registered to the private zone as A records pointing to their private IP addresses. When a virtual machine in a virtual network link with autoregistration enabled gets deleted, Azure DNS also automatically removes the corresponding DNS record from the linked private zone.

- **Forward DNS resolution is supported across virtual networks that are linked to the private zone**. For cross-virtual network DNS resolution, there's no explicit dependency such that the virtual networks are peered with each other. However, you might want to peer virtual networks for other scenarios (for example, HTTP traffic).

- **Reverse DNS lookup is supported within the virtual-network scope**. Reverse DNS lookup for a private IP associated to a private zone will return an FQDN that includes the host/record name and the zone name as the suffix.

Commands :-

Enable firewall to ping server each other :-

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

 # PowerShell command to install ISS

install IIS server role

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

remove default htm file

```
remove-item  C:\inetpub\wwwroot\iisstart.htm
```

Add a new htm file that displays server name

```
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from " +
$env:computername)
```

Powershell command to install google chrome

```
$LocalTempDir = $env:TEMP; $ChromeInstaller = "ChromeInstaller.exe"; (new-object
System.Net.WebClient).DownloadFile('http://dl.google.com/chrome/install/375.126/chrome_installer.ex
e', "$LocalTempDir\$ChromeInstaller"); & "$LocalTempDir\$ChromeInstaller" /silent /install;
$Process2Monitor =  "ChromeInstaller"; Do { $ProcessesFound = Get-Process | ?{$Process2Monitor -
contains $_.Name} | Select-Object -ExpandProperty Name; If ($ProcessesFound) { "Still running:
$($ProcessesFound -join ', ')" | Write-Host; Start-Sleep -Seconds 2 } else { rm
"$LocalTempDir\$ChromeInstaller" -ErrorAction SilentlyContinue -Verbose } } Until (!$ProcessesFound)
```