

Installing and Configuring DNS in Windows Server

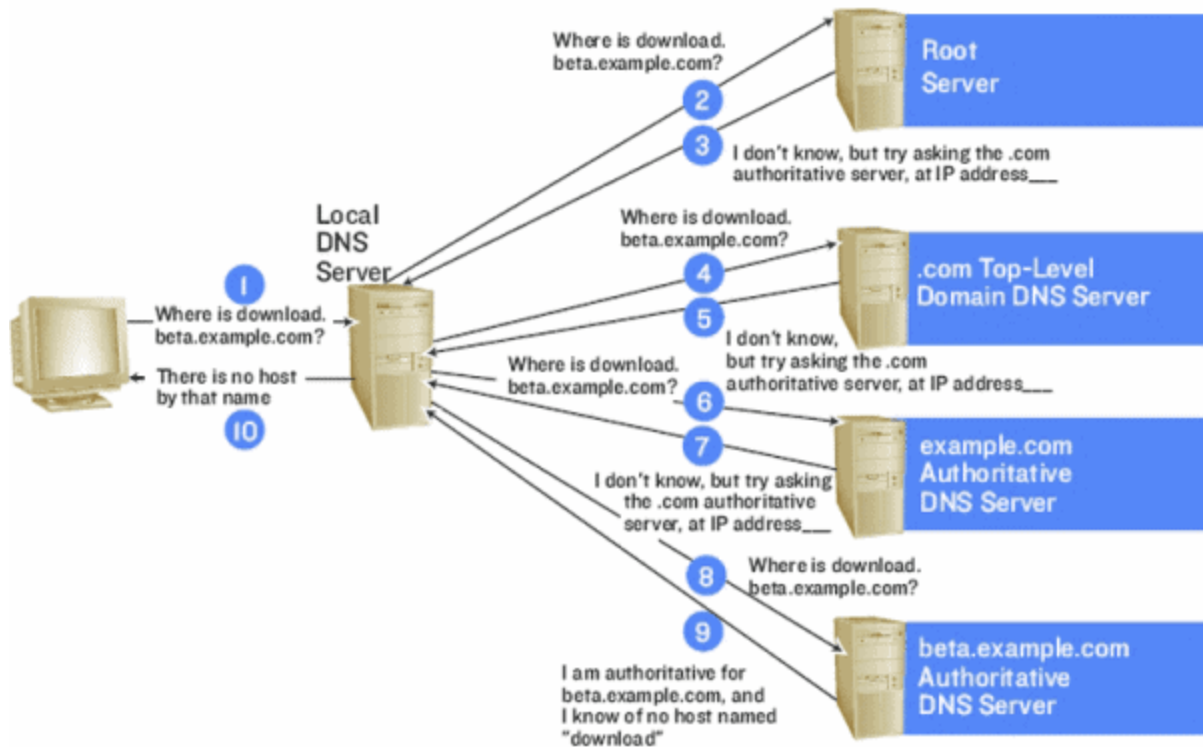
We know the Domain Name System and what it does, but we need to know how to install and configure DNS. For this article, we use the Windows Server 2012R2 DNS install process, which we also use for later builds like Windows Server 2016, 2019, and 2022

Overview of the Domain Name System

All in all, a [Domain Name](#) is a human readable version of an IP address. Well, an IP Address is what every computer on the internet uses to address itself when communicating with other computers via the TCP/IP network protocol. IP (v4) addresses, for example, look like a series of numbers and decimal points, such as **192.168.1.12**.

When [users](#) enter a domain name, such as www.infrasos.com, their browser communicates with a network of root domain name servers, which act as a reference book, providing the IP address associated with that [domain](#) name. The browser then communicates directly with the hosting server using that IP address.

Altogether, DNS serves as a go between, translating [user requests](#) into IP addresses. Without DNS, users need to memorize and enter long IP addresses when connecting to other websites, rather than simply typing in the website's name.



Prerequisites

Before configuring our DNS, we must have the following information:

- Our [domain](#) name.
- The IP address and hostname of each server that we want to provide name resolution for.

Additionally, before we configure our computer as a DNS, we need to verify that the following minimum conditions are proper:

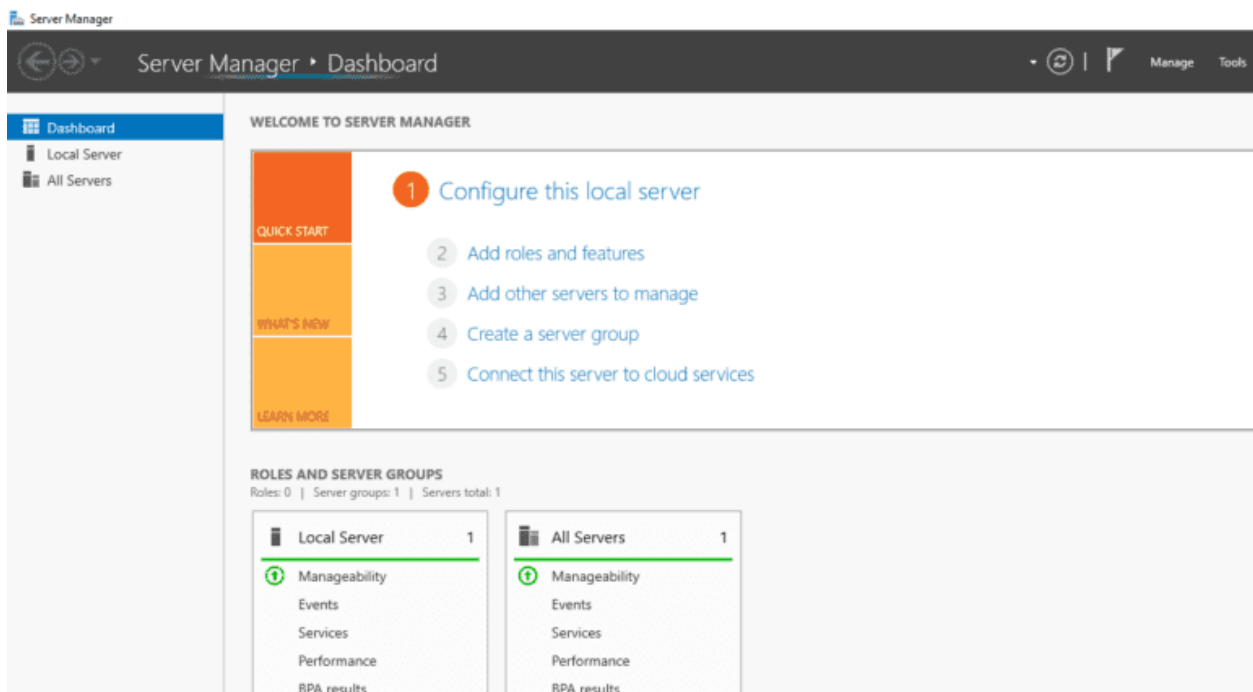
- A server running [Windows](#) Server 2012R2, 2016, 2019, or 2022 operating system and an open [Remote Desktop Protocol \(RDP\) 3389](#) port.
- A domain user with appropriate administrative privileges in configuring the DNS.
- Minimum of 4 GB of RAM and 2-core CPU.

Installing the DNS Server Role

Basically, installing the DNS Server Role in Windows Server is a simple process that allows you to configure and manage a DNS server for your [network](#). It involves adding the DNS server role to your Windows Server machine, configuring basic DNS settings, and creating and managing DNS records. First of all, log in as an [administrator user](#) to the Windows Server and follow the steps below to install the DNS server on our Windows Server:

Step 1: Launch the **Server Manager**, as illustrated below:

Step 2: Select **Add roles and features**.



Step 3: Press **Next**.

Before you begin

DESTINATION SERVER
CLOUD-JH209NLHC

Before You Begin

[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

< Previous

Next >

Install

Cancel

Step 4: Click on **Next** after selecting **Role based and feature based** installation.

Select installation type

DESTINATION SERVER
CLOUD-JH209NLHC

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

Step 5: Choose a server from the pool and press **Next**.

Select destination server

DESTINATION SERVER
CLOUD-JH209NLHC

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
CLOUD-JH209NLHC	208.117.85.195	Microsoft Windows Server 2022 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

Step 6: Pick the DNS server and click **Next**.

Select server roles

DESTINATION SERVER
CLOUD-JH209NLHC

Before You Begin

Installation Type

Server Selection

Server Roles

Features

DNS Server

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☒ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
 - ☐ Host Guardian Service
 - ☐ Hyper-V
 - ☐ Network Controller
 - ☐ Network Policy and Access Services
 - ☐ Print and Document Services
 - ☐ Remote Access
 - ☐ Remote Desktop Services
 - ☐ Volume Activation Services
 - ☐ Web Server (IIS)
 - ☐ Windows Deployment Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous

Next >

Install

Cancel

Step 7: Double check all settings before clicking the **Install** button to begin the installation.

Confirm installation selections

DESTINATION SERVER
CLOUD-JH209NLHC

Before You Begin

Installation Type

Server Selection

Server Roles

Features

DNS Server

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

DNS Server

Remote Server Administration Tools

Role Administration Tools

DNS Server Tools

[Export configuration settings](#)
[Specify an alternate source path](#)

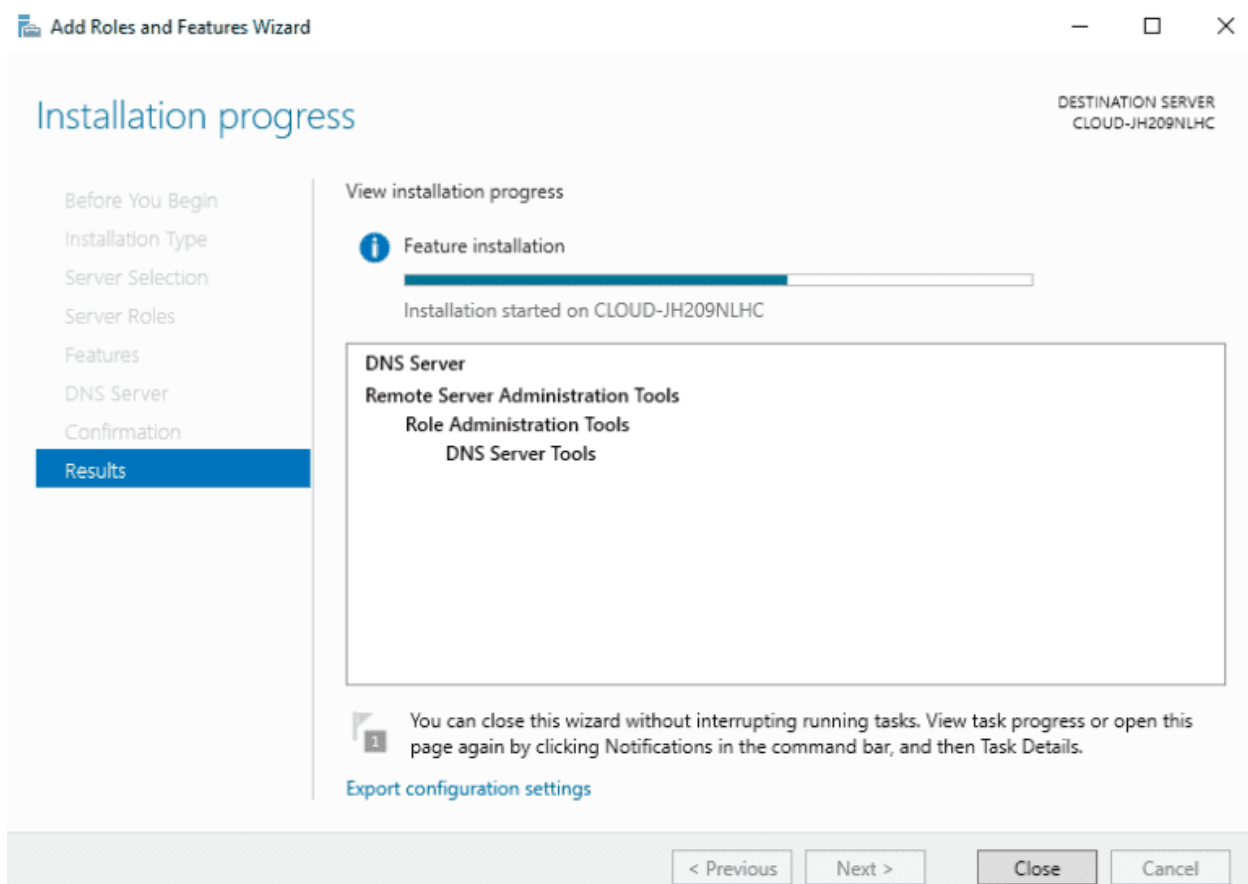
< Previous

Next >

Install

Cancel

Step 8: Allow some time for the installation to complete. Once done, click the **Close** to exit the installation wizard.



Installing the DNS Server Role Using PowerShell

Using [PowerShell](#), we automate the installation process, making it easier and more efficient to set up a DNS server for your [network](#). Here are the steps to install the DNS Server Role using [PowerShell](#) on Windows Server:

Step 1: Open Windows PowerShell as an admin by pressing the **Windows key + X** and selecting **Windows PowerShell (Admin)** from the menu.

Step 2: Use the [Install-WindowsFeature](#) command to install the **DNS Server Role**:

```
Install-WindowsFeature -Name DNS -IncludeManagementTools
```

Copy

Step 3: Press Enter to run the command. You see a message indicating that the installation process has started.

Step 4: Wait for the installation process to complete, which may take several minutes.

Step 5: After the installation is complete, use the [Get-WindowsFeature](#) command to confirm that the DNS Server Role has been installed:

```
Get-WindowsFeature -Name DNS
```

Copy

Step 6: You should see a message indicating that the DNS Server Role is installed, and the display name should be **DNS Server**.

As a result, using [PowerShell](#) to install the DNS Server Role saves time and effort compared to manually installing the role through the graphical user interface. Additionally, using PowerShell [allows](#) us to automate the installation process, making it easier to set up multiple DNS servers consistently and repeatedly.

In this part of the article about how to Install and Configure DNS Server on Windows Server we are configuring DNS server first.

Configuring the DNS Server

Now, that we have set up the DNS server role, we can use the DNS service inside the server. We need to create forward and reverse lookup zones to resolve the name to [IP address](#) and vice versa.

Configuring the Forward Lookup Zone

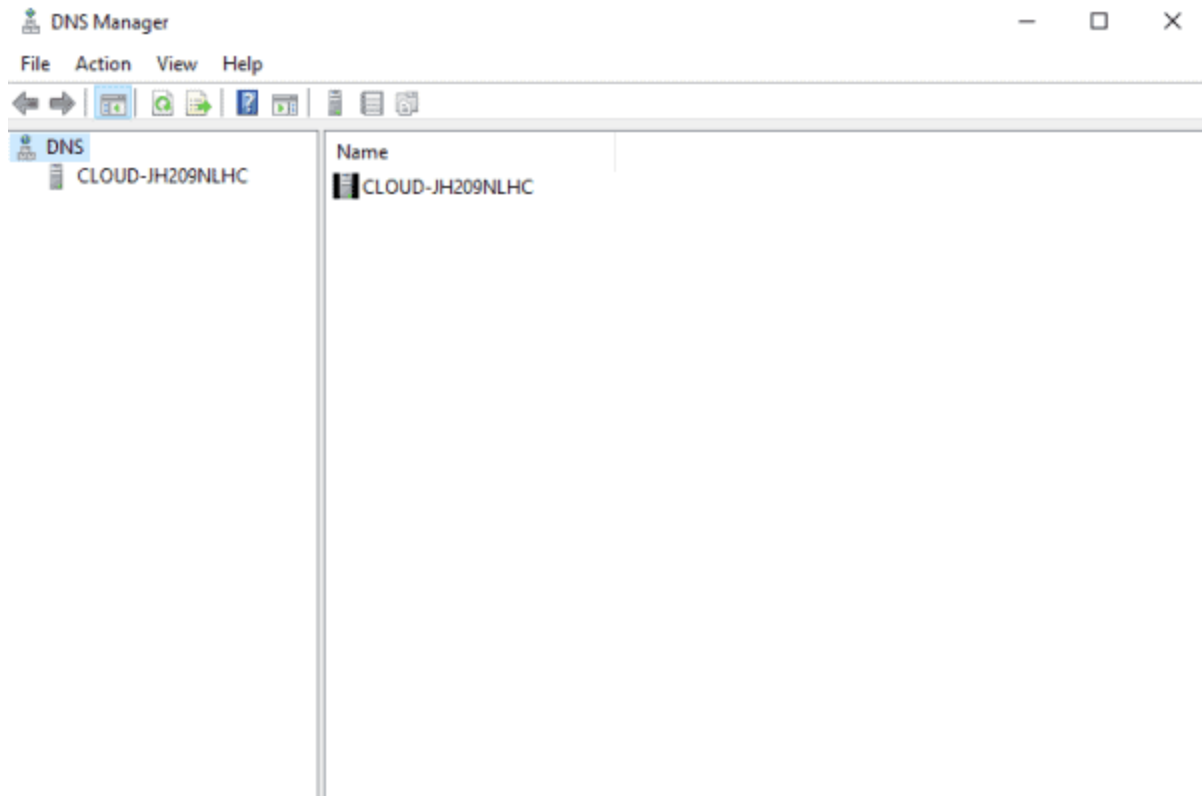
Evidently, a Forward Lookup Zone in DNS is a database of resource records that map domain names to IP addresses. Hence, we use it to resolve [host names](#) to IP addresses.

Certainly, the Forward Lookup Zone is vital because it enables clients to access network resources using [domain](#) names instead of IP addresses. This lookup zone makes it easier for [users](#) to remember and [access](#) network resources, and it helps improve the network's readability and maintainability.

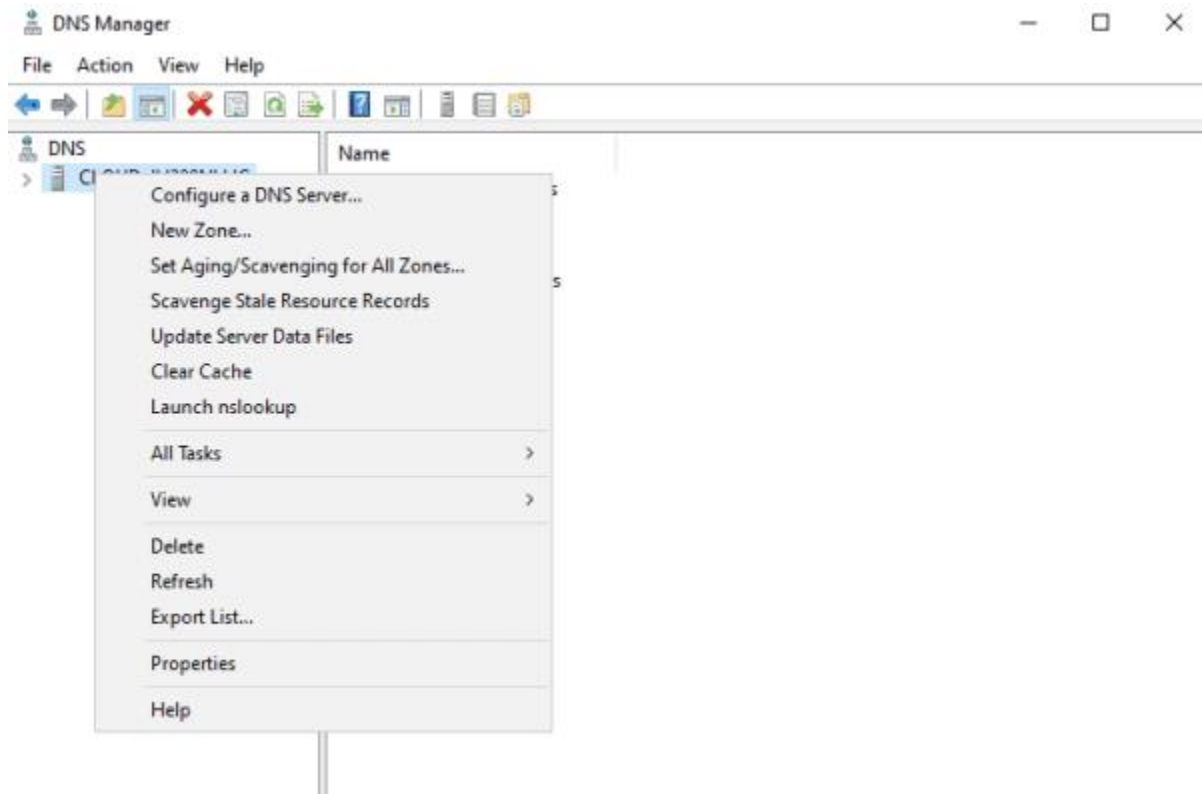
Steps

In order to create a forward lookup zone, follow the steps below:

Step 1: On the server manager, navigate to **Tools > DNS** to access the DNS manager, as shown below:

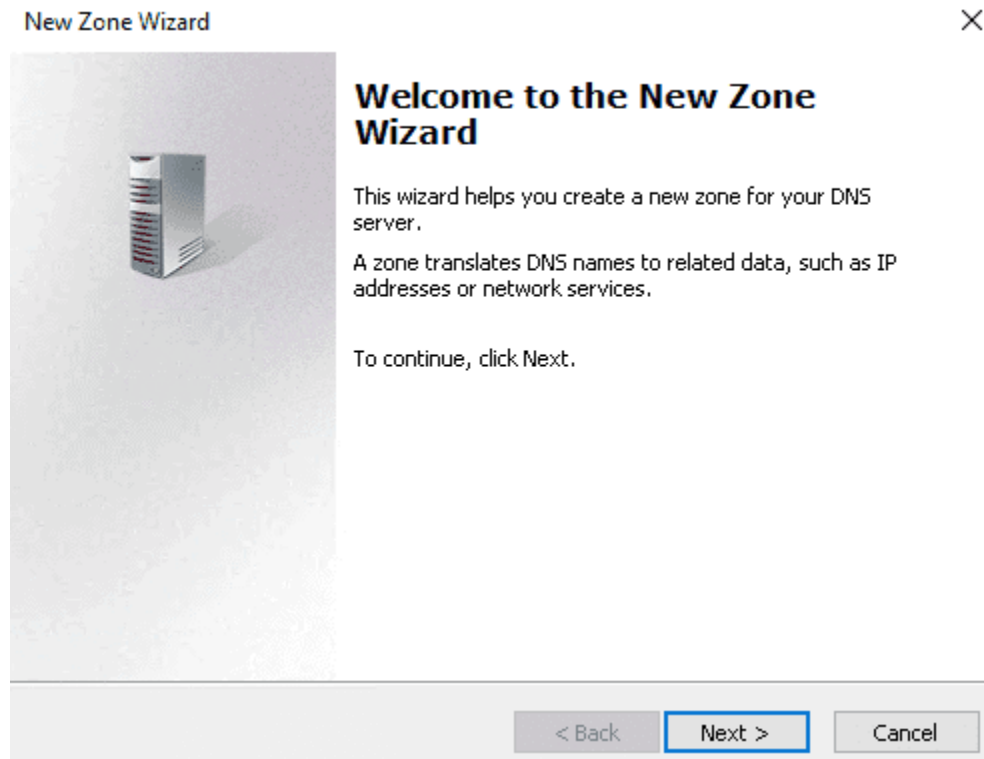


Step 2: Right click on the server name and select **Properties**.

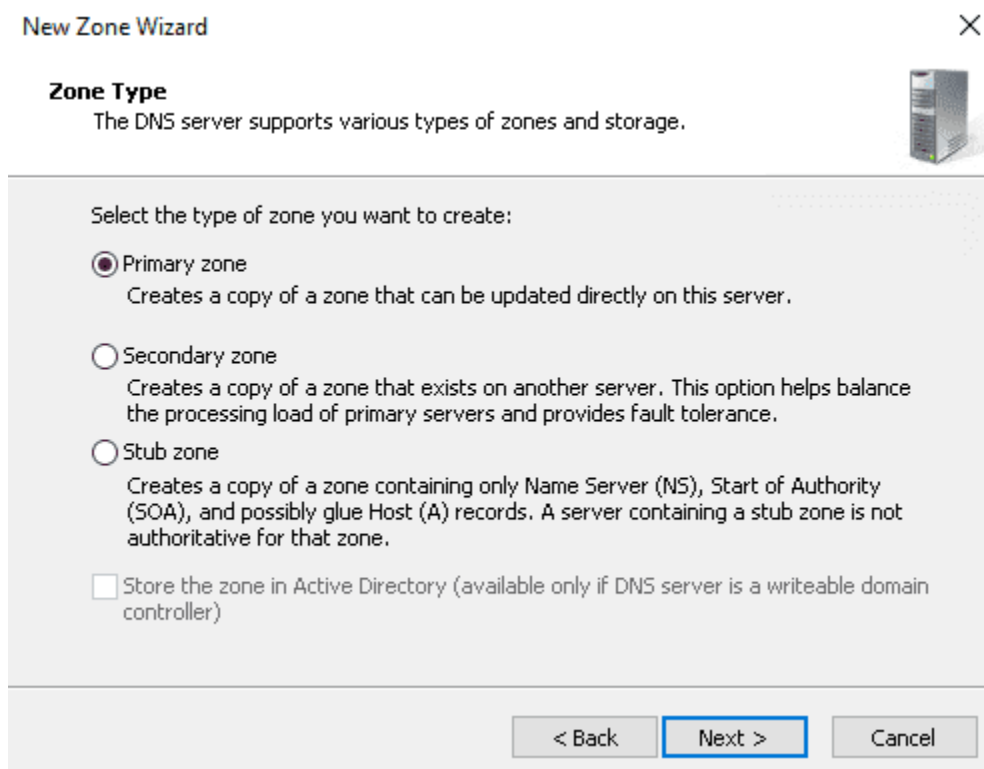


Step 3: Select the **New Zone** option.

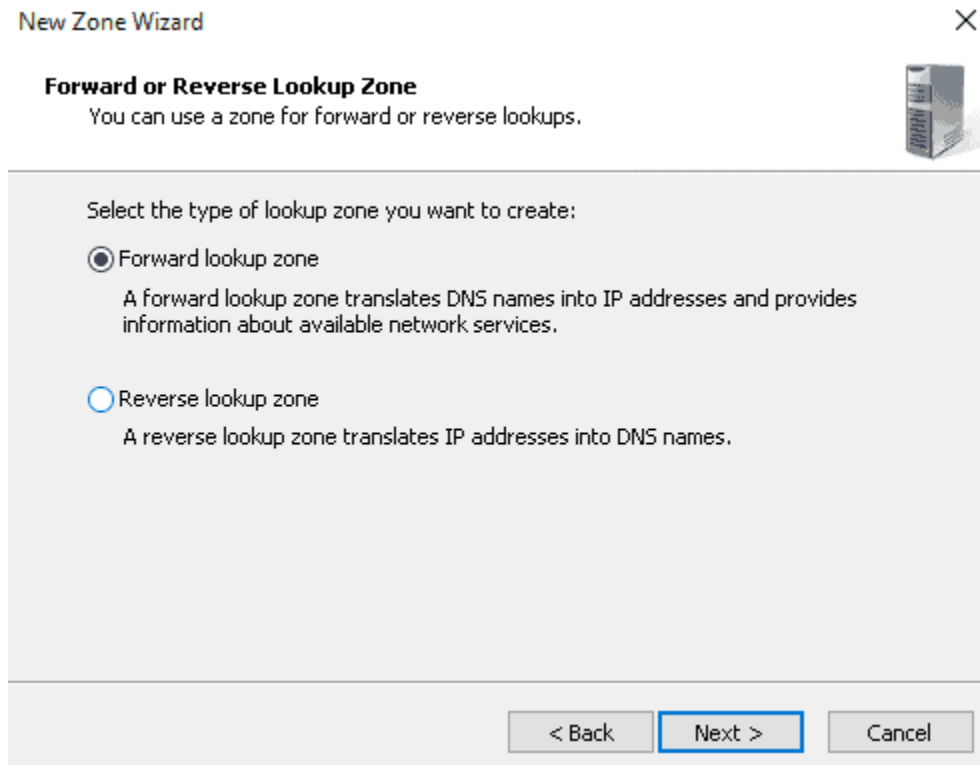
Step 4: Press Next.



Step 5: Choose the Primary zone and press Next.



Step 6: Click **Next** after selecting the **Forward lookup zone**.



The image shows a 'New Zone Wizard' dialog box with a close button (X) in the top right corner. The title bar is 'New Zone Wizard'. Below the title bar, the section is titled 'Forward or Reverse Lookup Zone' with a subtext 'You can use a zone for forward or reverse lookups.' and a server icon. The main area contains the instruction 'Select the type of lookup zone you want to create:'. There are two radio button options: 'Forward lookup zone' (which is selected) and 'Reverse lookup zone'. Below each option is a descriptive sentence. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

New Zone Wizard

Forward or Reverse Lookup Zone
You can use a zone for forward or reverse lookups.

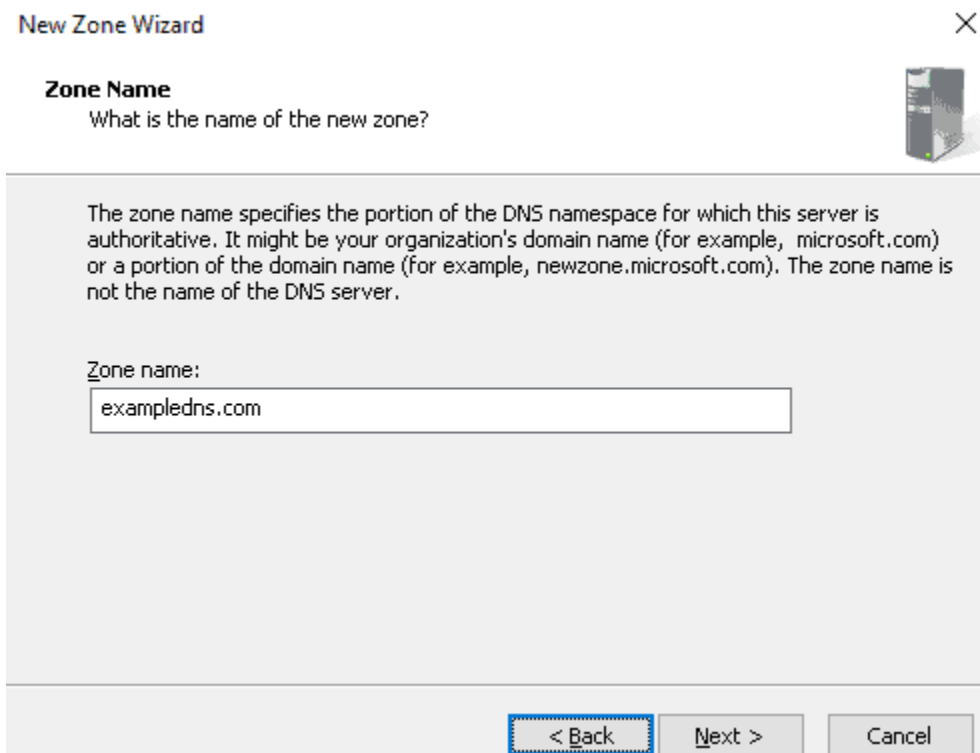
Select the type of lookup zone you want to create:

☒ Forward lookup zone
A forward lookup zone translates DNS names into IP addresses and provides information about available network services.

☐ Reverse lookup zone
A reverse lookup zone translates IP addresses into DNS names.

< Back **Next >** Cancel

Step 7: Enter the name of our zone and press **Next**.



The image shows a 'New Zone Wizard' dialog box with a close button (X) in the top right corner. The title bar is 'New Zone Wizard'. Below the title bar, the section is titled 'Zone Name' with a subtext 'What is the name of the new zone?' and a server icon. The main area contains a paragraph explaining the zone name. Below this is a label 'Zone name:' followed by a text input field containing 'exampledns.com'. At the bottom right, there are three buttons: '< Back' (highlighted with a blue border), 'Next >', and 'Cancel'.

New Zone Wizard

Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:
exampledns.com

< Back Next > Cancel

Step 8: Choose “**Create a file with the file name**” and press **Next**.

New Zone Wizard ✕

Zone File

You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

exampledns.com.dns

☐ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back Next > Cancel

Step 9: Check the box next to “Do not allow dynamic update” and click **Next**.

New Zone Wizard ✕


Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

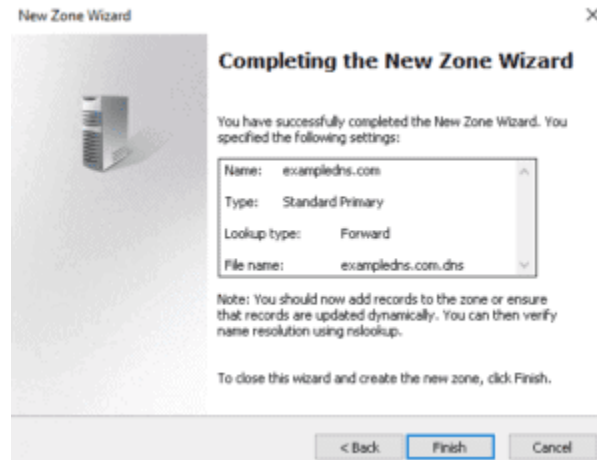
☐ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☒ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

Step 10: Press the **Finish** button.



Next, with Install and Configure DNS Server on Windows Server we configure Reverse Lookup Zone.

Configuring the Reverse Lookup Zone

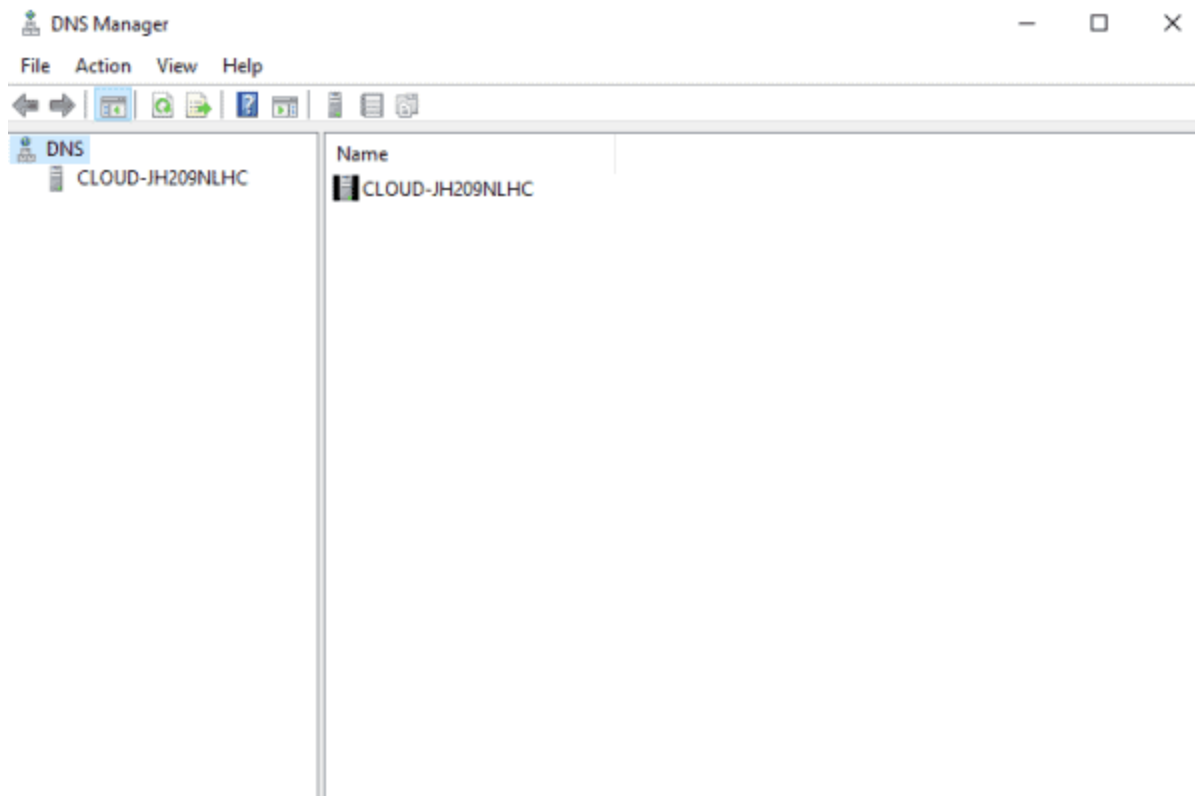
Following, a Reverse Lookup Zone in DNS is a database of resource records that map IP addresses to [host names](#). By all means, we use this lookup zone to resolve IP addresses to hostnames.

Further, a Reverse Lookup Zone is different from the Forward Lookup Zone. In that it maps IP addresses to host names, while the Forward Lookup Zone maps host names to IP addresses. Additionally, the Reverse Lookup Zone is typically less frequently used than the Forward Lookup Zone, as clients are more likely to access [network resources](#) using host names rather than IP addresses.

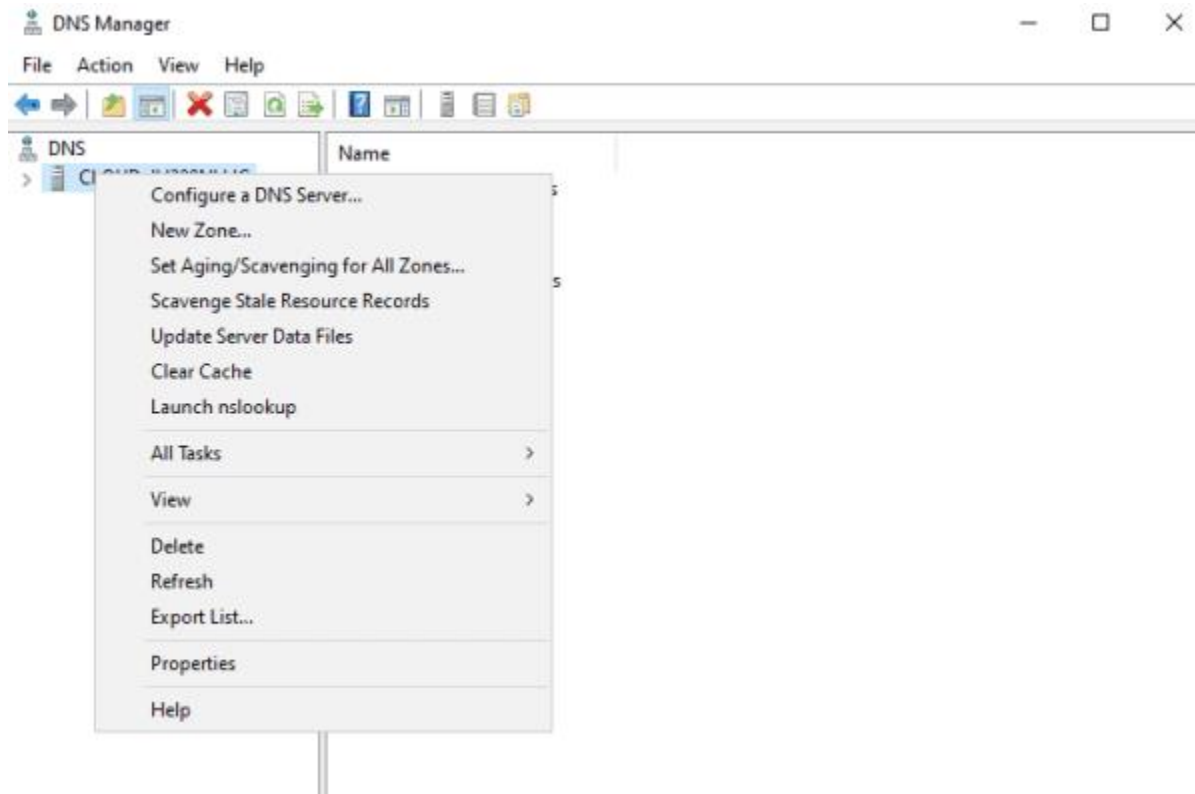
Steps

Indeed, to create a forward lookup zone, follow the steps below:

Step 1: On the server manager, navigate to **Tools > DNS** to access the DNS manager:

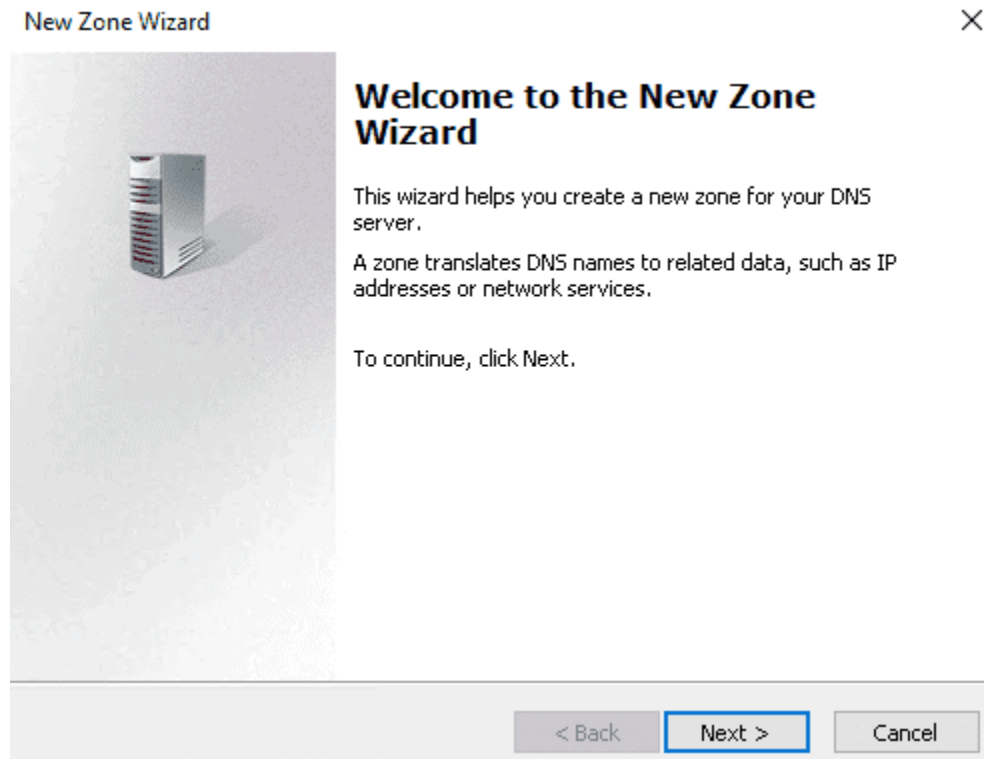


Step 2: Right click on the server name and select **Properties**.

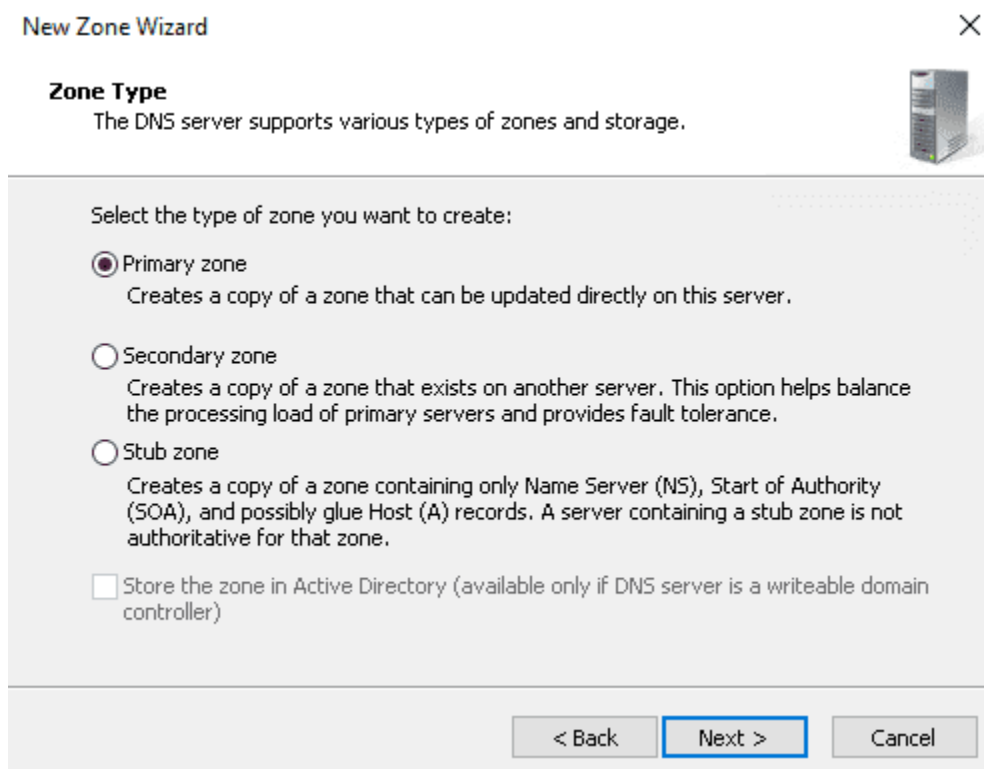


Step 3: Here, select the **New Zone** option.

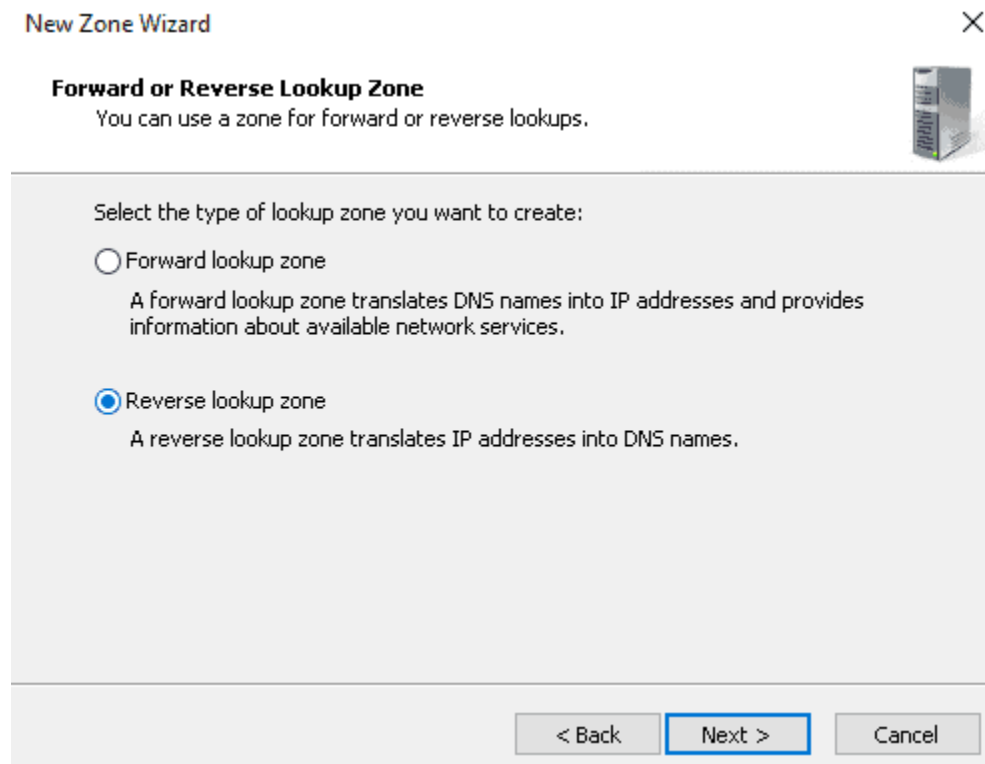
Step 4: Press Next.



Step 5: Now, choose the Primary zone and press Next.



Step 6: From this step forward, the setup is different from our previous section. Next, click **Next** after selecting the **Reverse lookup zone**.



The image shows a 'New Zone Wizard' dialog box with a close button (X) in the top right corner. The title bar is 'New Zone Wizard'. Below the title bar, the section is 'Forward or Reverse Lookup Zone' with a subtext 'You can use a zone for forward or reverse lookups.' and a server icon. The main area contains the instruction 'Select the type of lookup zone you want to create:' followed by two radio button options. The first option is 'Forward lookup zone' with a description 'A forward lookup zone translates DNS names into IP addresses and provides information about available network services.' The second option is 'Reverse lookup zone' (selected) with a description 'A reverse lookup zone translates IP addresses into DNS names.' At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

New Zone Wizard

Forward or Reverse Lookup Zone
You can use a zone for forward or reverse lookups.

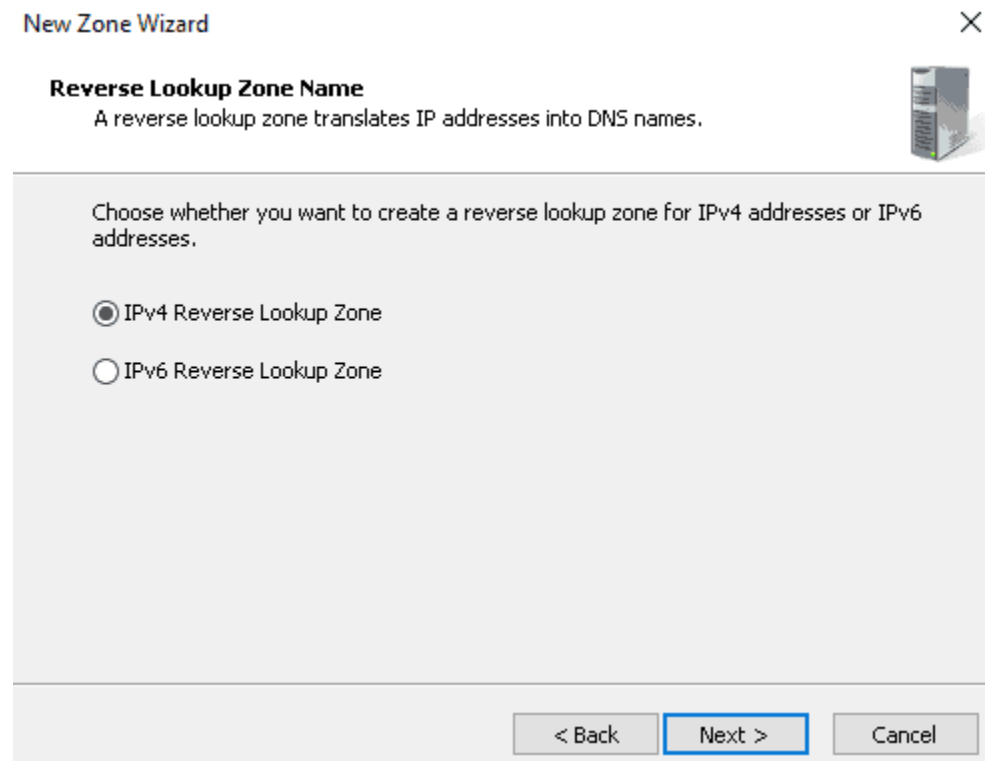
Select the type of lookup zone you want to create:

☐ Forward lookup zone
A forward lookup zone translates DNS names into IP addresses and provides information about available network services.

☒ Reverse lookup zone
A reverse lookup zone translates IP addresses into DNS names.

< Back Next > Cancel

Step 7: After, select **IPv4 Reverse Lookup Zone** and click on **Next**.



The image shows a 'New Zone Wizard' dialog box with a close button (X) in the top right corner. The title bar is 'New Zone Wizard'. Below the title bar, the section is 'Reverse Lookup Zone Name' with a subtext 'A reverse lookup zone translates IP addresses into DNS names.' and a server icon. The main area contains the instruction 'Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.' followed by two radio button options. The first option is 'IPv4 Reverse Lookup Zone' (selected) and the second is 'IPv6 Reverse Lookup Zone'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

☒ IPv4 Reverse Lookup Zone

☐ IPv6 Reverse Lookup Zone

< Back Next > Cancel

Step 8: Define your network ID and click **Next**.

New Zone Wizard ✕

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ **Network ID:**

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ **Reverse lookup zone name:**

Step 9: Further, choose “**Create a file with the file name**” and press **Next**.

New Zone Wizard ✕

Zone File
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ **Create a new file with this file name:**

☐ **Use this existing file:**

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

Step 9: Please check the box next to “**Do not allow dynamic update**” and click **Next**.

New Zone Wizard



Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.



Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☐ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
- ☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☒ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back

Next >

Cancel

Step 10: In sum, press the **Finish** button.

New Zone Wizard



Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name:	85.117.208.in-addr.arpa
Type:	Standard Primary
Lookup type:	Reverse
File name:	85.117.208.in-

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

< Back

Finish

Cancel

Configuring DNS Records

Moreover, DNS records are essential for several reasons:

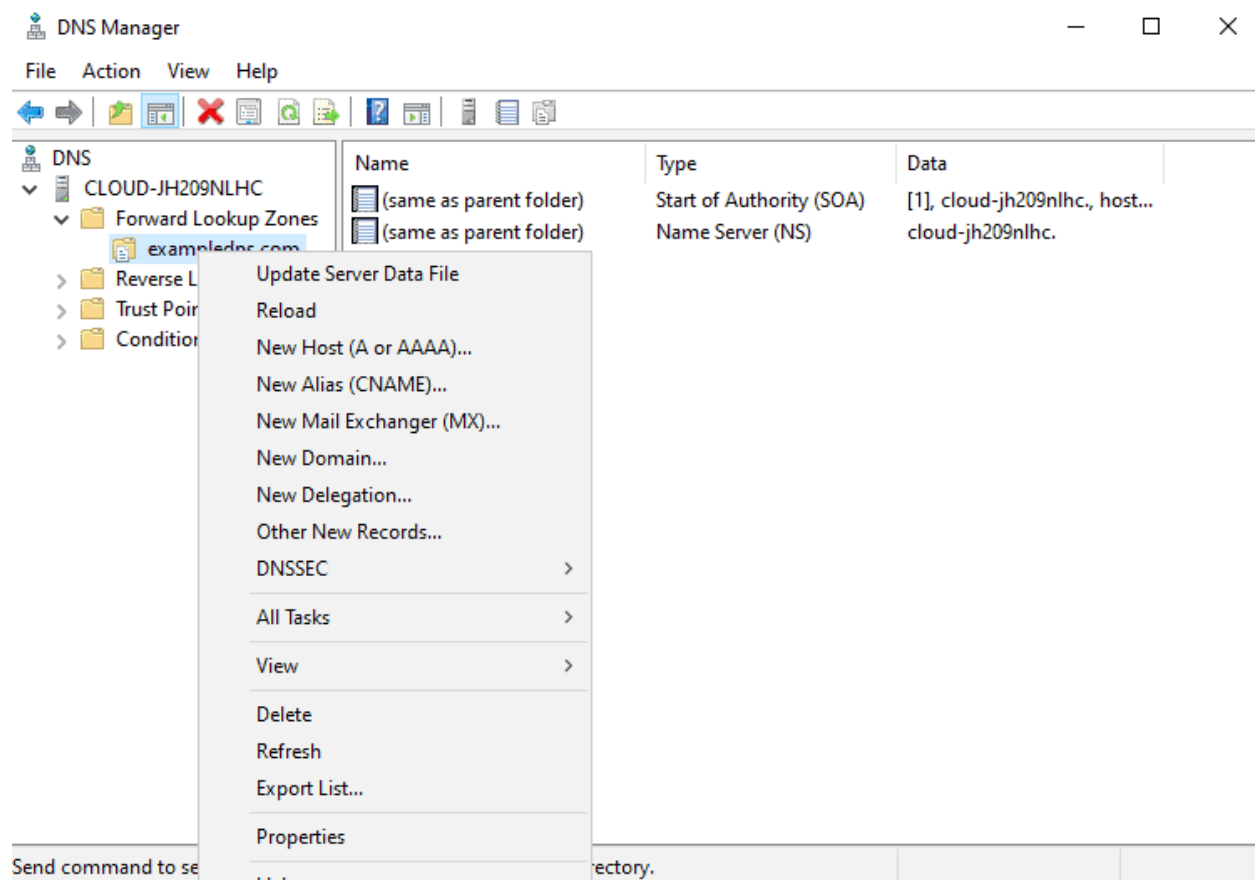
1. **Domain name resolution:** In short, we use DNS records to [map domain](#) names to IP addresses, allowing clients to access network resources using human readable names rather than IP addresses.
2. **Network functionality:** Properly configured DNS records are [critical](#) for ensuring network services and applications function correctly.
3. **Network security:** In similar fashion, we use DNS records to [secure](#) our network by providing information about which IP addresses correspond to our domain names. We use this information to block [malicious traffic](#) and improve network [security](#).
4. **Load balancing:** By creating multiple A records for the same hostname and assigning different IP addresses to each record, we distribute incoming traffic across multiple servers, improving the [performance](#) and reliability of our [network](#).
5. **Management and administration:** In this case, DNS records are managed and updated centrally, making organizing and maintaining our network easier.

Overall, DNS records are a fundamental part of the functioning of the internet and are critical for ensuring that domain names are resolved to IP addresses. That network services and [applications](#) work correctly and that networks are [secure](#) and reliable.

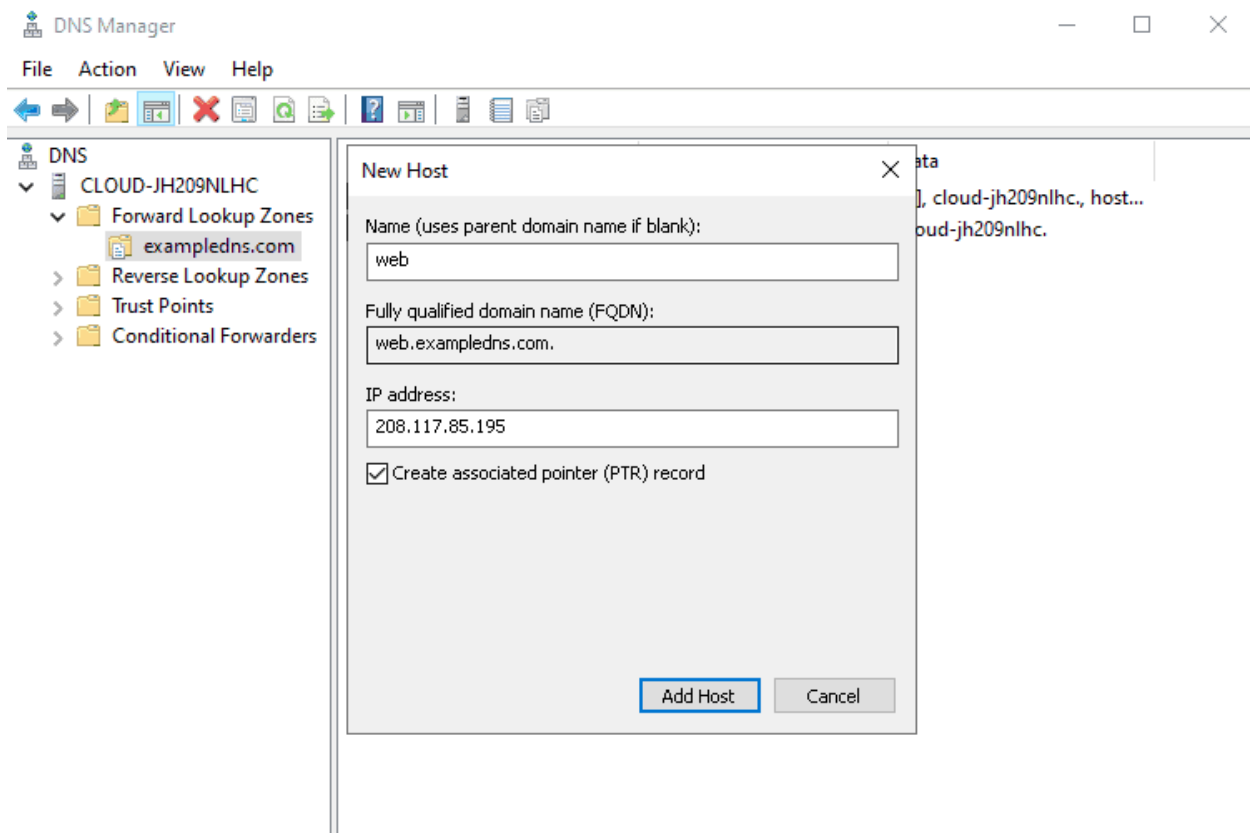
Steps

Please follow the below steps to add A and PTR records to DNS:

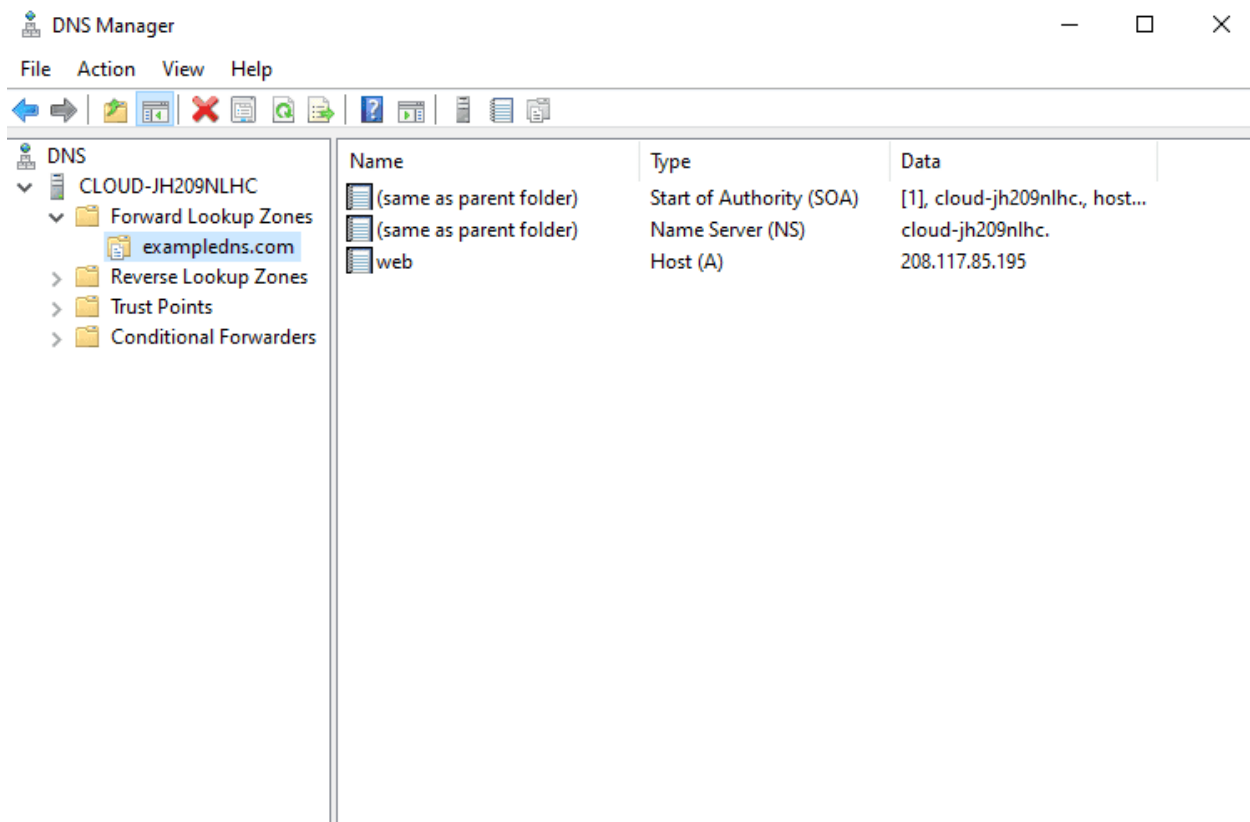
Step 1 : On the DNS manager, right click on the **forward lookup** zone.



Step 2: Click on the **New Host (A or AAAA)**.



Step 3: Provide the host's parent domain name and IP address, select **“Create associated pointer record”** and then click on the **Add Host** button.



When creating a zone in [Windows](#) Server DNS, the Start of Authority (**SOA**) and Name Server (**NS**) records are automatically created for several reasons:

1. **Start of Authority (SOA) Record:** The SOA record defines the start of a DNS zone and provides information about the zone itself. This record is required for all zones and is used to identify the authoritative source of information for the zone. In addition, the SOA record contains essential information, such as the primary DNS server for the zone, the [email](#) address of the person responsible for the zone, and the refresh and retry intervals for the zone.
2. **Name Server (NS) Record:** The NS record identifies the authoritative DNS servers for a particular zone. These servers serve DNS information for the zone and resolve DNS queries for the domain. The NS record is also used to delegate subdomains to other DNS servers.

Given that, the process is streamlined and simplified by automatically creating the [SOA](#) and NS records when creating a zone in Windows Server DNS, ensuring that the required information for the zone is present and accurate. Particularly, this helps to ensure that the zone functions correctly and that the network resolves DNS queries for the domain.

Other Types of DNS Records

In the above example, we created **A** (forward lookup) and **PTR** (reverse lookup) records. However, these are only some records available when managing the DNS. Here are some examples below:

Type of Record	Definition
A (Address)	Example, that maps a host name to an IPv4 address
AAAA (IPv6 Address)	Another, that maps a host name to an IPv6 address
MX (Mail Exchange)	Specifies the mail servers responsible for a specific domain name
CNAME (Canonical Name)	Following example, that maps an alias to a true or canonical domain name
NS (Name Server)	Specifies the name servers for a specific domain name
PTR (Pointer)	Here, it maps an IPv4 or IPv6 address to a host name (reverse DNS lookup)
SRV (Service)	Similarly, it specifies the host and port for a specific service for a domain name
TXT (Text)	Stores text-based information such as SPF records, email routing information, or information

Note: This table lists the most common types of [DNS](#) records, but many other types are available. In detail, the specific records we need depends on our network's requirements and the services we want to provide.

Verifying DNS Records

Now, we need to test whether the DNS name resolution works. First, open our command line interface and run the **nslookup** command:

```
nslookup
```

Copy

We should see the name of the Primary DNS server that our machine is currently connected to:

```
Default Server:  web.exampledns.com
```

```
Address:  208.117.85.195
```

Copy

In fact, now please type the Fully Qualified Domain Name (FQDN) of our added host:

```
sample.exampledns.com
```

Copy

We should see the name to IP address resolution in the following output. A valid output means that our forward lookup is working:

```
Server:  web.exampledns.com
```

```
Address:  208.117.85.195
```

```
Name:  sample.exampledns.com
```

```
Address:  208.117.85.1
```

Copy

Subsequently, next try typing, the IP address of our added host:

```
208.117.85.1
```

Copy

And we should see the IP address to name resolution in the following output which also means our reverse lookup is functioning:

```
Server:  web.exampledns.com
```

```
Address:  208.117.85.195
```

```
Name:  sample.exampledns.com
```

```
Address:  208.117.85.1
```

Copy

Thank you for reading the article about how to Install and Configure DNS Server on Windows Server. We shall conclude the article now.

Install and Configure DNS Server on Windows Server Conclusion

In conclusion, installing and configuring DNS on Windows Server is critical for any organization that wants to provide reliable and secure domain name resolution services. Finally, DNS is a critical component of the [internet](#). Therefore, it is vital to ensure that we resolve domain names to IP addresses, that network services and [applications](#) work correctly, and that networks are [secure](#) and reliable.

By configuring DNS in Windows Server, we improve the [management](#) and administration of our network, as well as provide enhanced security and reliability. Installing and configuring DNS in Windows Server is straightforward. We use the graphical user interface or the command line to configure DNS servers and create and manage DNS records.