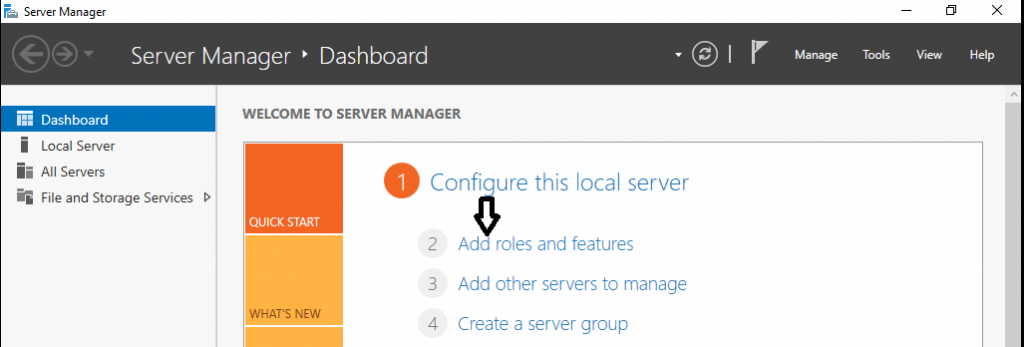
**Install and Configure DNS on Windows Server 2019**

**Prerequisites**

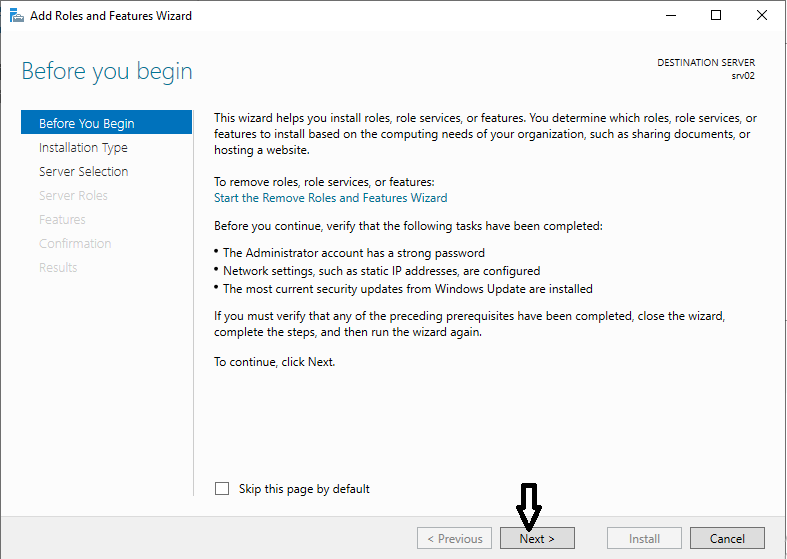
1. Server OS (Windows server 2019)
2. Administrator Account
3. A Static IP address is configured(We are going to use IP address 10.0.2.2 in our lab)

**Install Windows DNS Server**

Step1: Open the server manager dashboard and Click add roles and features.



Step 2: Click on Next



Step 3: Choose Role-based or feature-based installation and click Next.

Graphical user interface, text, application

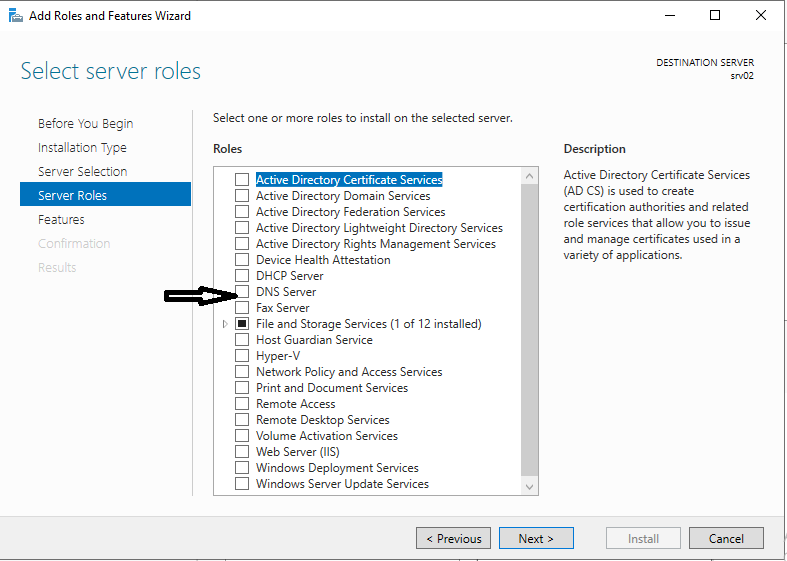
Description automatically generated

Step 4: Choose destination server for DNS role and click Next

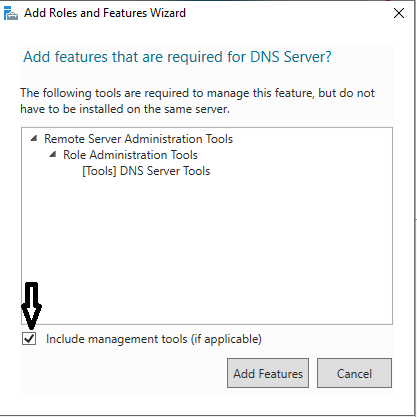
Graphical user interface, text, application, email

Description automatically generated

Step 5: Put the Check on the DNS server for DNS Server Role Installation



Step 6: Add features that are required for the DNS server including management tools.

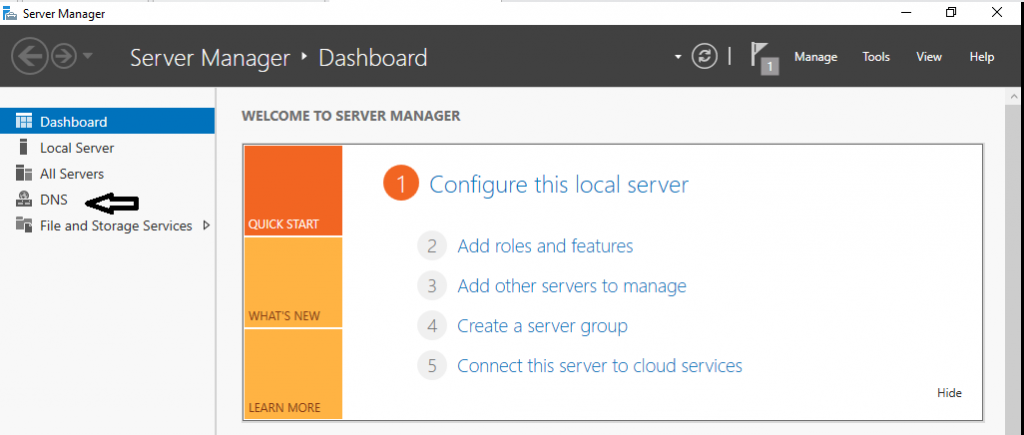


Step 7: After adding of required features it installs the DNS server with a succeeded message.

Graphical user interface, text, application

Description automatically generated

Step 8: After DNS Server Installation you can access the DNS server from Server Manager or from Administrative Tools option in windows Program.



**Creating Forward Lookup Zone**

**Step 1**. Open DNS management console from server manager or from Windows Administrative Tools.

Graphical user interface, application

Description automatically generated

**Step 2**. In DNS manager console, look for your server’s name on the left. Right-click on the server’s name and choose “Configure a DNS Server”

Graphical user interface, text, application

Description automatically generated

**Step3** Follow the DNS Server configuration wizard, We will choose “Create a forward lookup zone” .

Graphical user interface, text, application

Description automatically generated

We choose “This server maintains the zone”.

Graphical user interface, text, application, email

Description automatically generated

We will name our zone as “netserv.edu.au”.

Graphical user interface, text, application, email

Description automatically generated

A new zone file “netserv.edu.au.dns” will be created in C:\Windows\System32\dns directory.

Graphical user interface, text, application, email

Description automatically generated

Do not allow dynamic updates for our zone.

Graphical user interface, text, application, email

Description automatically generated

Use ipconfig /all to check your VM’s DNS Server IP address for Ethernet0, configure this IP address as forwarder, my VM use 192.168.70.2, your DNS server IP address can be different.

Graphical user interface, text, application, email

Description automatically generated

We want to see the green tick for this forwarder address.

Graphical user interface, text, application, email

Description automatically generated

Finish the DNS server configuration wizard.

Graphical user interface, application

Description automatically generated

**Step 4** Set up DNS server properties

Right click the DNS server’s name, choose properties.

Graphical user interface, text, application

Description automatically generated

Select only 10.0.2.2 interface to listen for DNS queries.

Graphical user interface, text, application

Description automatically generated

**Step 5** Create the forward lookup zone file.

Click the forward lookup zones, then “netserv.edu.au”, we can see the zone file information, change the ns record properties according to our lab requirement.

Graphical user interface, text, application

Description automatically generated

Edit the FQDN to ns. With IP address 10.0.2.2

Graphical user interface, text, application, email

Description automatically generated

Zone transfer to any server

Graphical user interface, text, application, email

Description automatically generated

**Step6** Add more entries to the Zone file

Right click the Zone name, then add the zone record according to the lab manual.

* New host (A): ns with IP address 10.0.2.2
* New host (A): mail with IP address 10.0.2.2
* New Mail Exchanger (MX): leave host blank and the FQDN should be mail
* New host (A): site with IP address 10.0.2.2
* New Alias (CNAME): www and FQDN site

Graphical user interface, application

Description automatically generated

Now the zone record look like the following

Graphical user interface, text, application, email

Description automatically generated

Right click the DNS domain, choose “**New delegation**” to Create a delegation for the it.netserv.edu.au domain.

**Note about Delegation**: For a DNS server to answer queries about any name, it must have a direct or indirect path to every zone in the namespace. These paths are created by means of delegation. A delegation is a record in a parent zone that lists a name server that is authoritative for the zone in the next level of the hierarchy. Delegations make it possible for servers in one zone to refer clients to servers in other zones.

Graphical user interface, text, application, email

Description automatically generated

Click the “Add” to enter the name server record. We will use Linux server. The Linux machine is not configured yet, so you will see the validation timed out.

Graphical user interface, text, application, email

Description automatically generated

Now right click the server to “update Server Data File”.

Graphical user interface, text, application, email

Description automatically generated

Now restart the DNS server:

From “Tools” select “Service”, find the DNS Server to restart it.

Graphical user interface, text

Description automatically generated

**Step 7**. Now we can test the DNS configuration.

Use nslookup to set the DNS server as 10.0.2.2, domain=netserv.edu.au, query type to A record, then start the query

Text

Description automatically generated

**Step 8** add DNS Reverse Lookup Zone

Open zone manager, right click the “Reverse Lookup Zones”, select a new zone.

Graphical user interface, application

Description automatically generated

Then follow the configuration wizard, select “Primary zone”, “IPv4 Reverse lookup Zone”, enter the Network ID.

Graphical user interface, text, application, email

Description automatically generated

Click “next”, then “next”, “finish”

Graphical user interface, text, application, email

Description automatically generated

Select the reverse zone, edit the Name Server priority

Graphical user interface, text, application, email

Description automatically generated

Now create a PTR record

Graphical user interface, application

Description automatically generated

# Set Up Private DNS Servers with BIND on CentOS 8

# Prerequisites

* Access to the root user account (or access to an admin account with root privileges)
* Static IP address (we are going to use 10.0.2.3)

## Step 1: Install BIND DNS Server

By default, the bind package is available in the CentOS 8 standard repository. You can install it by running the following command:

dnf install bind

## Step 2: Configure BIND DNS Server

By default, the BIND server is listening on localhost only. So you will need to configure it to listen on all network interfaces. You can configure it by editing the file /etc/named.conf:

The following sections may be used in /etc/named.conf:

**options** — Assigns values to many assorted options, including the use of forwarders, the location of the named working directory, the names of the various files, and much more.

We are going to modify the following lines in this section to allow any host and add a forwarder:

options {

listen-on port 53 { any; };

listen-on-v6 port 53 { ::1; };

directory "/var/named";

……

allow-query { any; };

forwarders {

10.0.2.2;

};

Note: for our forwarder to work we need to disable our Linux bind server from checking DNSSEC data.(DNS security extensions). In the /etc/named.conf file, look for the following lines, and update “yes” to “no” as shown below:

dnssec-enable no;

dnssec-validation no;

**zone "<zone-name>"** — Specifies particular zones for which this nameserver is authoritative. The zone statement is primarily used to specify the file containing the zone's configuration and pass certain options about that zone to named that override other global option statements used in /etc/named.conf.

We are going to add the following zone information in the /etc/named.conf file. A Forward Zone is used to resolve the hostname to IP address while a Reverse Zone is used to resolve the IP address to hostname. Generally, all normal DNS queries are forward lookup queries

//Forward Zone

zone "it.netserv.edu.au" IN {

type master;

file "it.netserv.edu.au.zone";

};

//Reverse Zone

zone "2.0.10.in-addr.arpa" {

type master;

file "2.0.10.in-addr.arpa.zone";

};

Save and close the file when you are finished.

## Step 3: Create Forward and Reverse Zone Files

Zone files, which contain information about a particular namespace, are stored in the named working directory. By default, this is /var/named. Each zone file is named according to the file option data in the zone statement, usually in a way that relates to the domain in question and identifies the file as containing zone data, such as it.netserv.edu.au.zone.

Each zone file may contain directives and resource records. **Directives** tell the nameserver to do a certain thing or apply a special setting to the zone. **Resource records** define the parameters of the zone, assigning an identity within the zone's namespace to particular systems. Directives are optional, but resource records are required to provide nameservice to that zone. All directives and resource records should go on their own lines.

Let’s create a forward and reverse zone files defined in the previous step. By default, all zone lookup files are located inside /var/named directory.

First, create a forward zone file with the following command:

vim /var/named/it.netserv.edu.au.zone

Add the following lines:

$TTL 1D

@ IN SOA ns.it.netserv.edu.au. root.it.netserv.edu.au. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

IN NS ns.it.netserv.edu.au.

IN MX 10 mail

IN A 10.0.2.3

site IN A 10.0.2.3

mail IN A 10.0.2.3

ns IN A 10.0.2.3

wwww IN CNAME site

ftp IN CNAME site

Create a reverse forward zone file with the following command:

vim /var/named/2.0.10.in-addr.arpa.zone

Add the following lines:

$TTL 1D

@ IN SOA ns.it.netserv.edu.au. root.it.netserv.edu.au. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

IN NS ns.it.netserv.edu.au.

2 IN PTR site.netserv.edu.au.

3 IN PTR site.it.netserv.edu.au.

Zone file resource records contain columns of data, separated by whitespace, that define the record. All zone file resource records are assigned a particular type, which designates the record's purpose. The following types of resource records are the most commonly used:

**SOA** — Start Of Authority record, proclaiming important authoritative information about the namespace to the nameserver.

Located after the directives, an SOA record is the first resource record in a zone file.

@ IN SOA *<primary-name-server>* *<hostmaster-email>* (

*<serial-number>*

*<time-to-refresh>*

*<time-to-retry>*

*<time-to-expire>*

*<minimum-TTL> )*

Note: The serial number is incremented every time you change the zone file so that named will know that it should reload this zone.

**A** — Address record, which specifies an IP address to assign to a name.

|  |
| --- |
| *<host>* IN A *<IP-address>* |

If the <host> value is omitted, then an A record points to a default IP address for the top of the namespace. This system will be the target of all non-FQDN requests.

**CNAME** — Canonical name record, which tells the nameserver that one name is also known as another.

|  |
| --- |
| *<alias-name>* IN CNAME *<real-name>* |

**MX** — Mail eXchange record, which tells where mail sent to a particular namespace controlled by this zone should go.

|  |
| --- |
| IN MX *<preference-value>* *<email-server-name>* |

The *<preference-value>* allows you to numerically rank the email servers you would prefer to receive email for this namespace.

**NS** — NameServer record, which announces the authoritative nameservers for a particular zone.

IN NS *<nameserver-name>*

The *<nameserver-name>* should be a FQDN.

**PTR** — PoinTeR record, designed to point to another part of the namespace.

PTR records are primarily used for reverse name resolution, as they point IP addresses back to a particular name.

|  |
| --- |
| *<last-IP-digit>* IN PTR *<FQDN-of-system>* |

**Note:** remember to change the zone file ownership to “named” after modifying the zone file.

chgrp named it.netserv.edu.au.zone

chgrp named 2.0.10.in-addr.arpa.zone

Save and close the file when you are finished.

## Step 4: Verify DNS Configuration

After configuring all zone files, you will need to verify the configuration files.

First, validate the main configuration file with the following command:

named-checkconf /etc/named.conf

If everything is fine, you don’t see any error.

Next, verify the forward zone file with the following command:

named-checkzone it.netserv.ecud.au /var/named/it.netserv.edu.au.zone

You should get the following output:

zone it.netserv.ecud.au/IN: loaded serial 0

OK

Next, verify the reverse zone file with the following command:

named-checkzone 2.0.10.in-addr.arpa.zone /var/named/2.0.10.in-addr.arpa.zone

You should get the following output:

zone 1.168.192.in-addr.arpa/IN: loaded serial 3

OK

Finally, start the BIND service and enable it to start at system reboot:

systemctl start named

systemctl enable named

## Step 5: Configure Firewall

Next, you will need to create a firewall rule for port 53 to allow DNS queries from client machines. You can create it with the following command:

firewall-cmd --permanent --add-port=53/udp

Next, reload the filewall service to apply the changes:

firewall-cmd --reload

## Step 5: Verify DNS Server

At this point, the BIND DNS server is installed and configured. It’s time to check whether it is working or not.

dig @localhost site.it.netserv.edu.au

dig @localhost it.netserv.edu.au soa

dig @localhost -x 10.0.2.2

Congratulations! you have successfully set up a private DNS server with BIND on CentOS 8.