

# DNS and DHCP in a Windows server.

—

Carlos Gerez

# cit470

## Task: Diagram

### Team 10 Layer 3: outside zones' public IPv4 address assignments

public space (IPv4 subnet ID)	router	firewall (dynamic NAT)	static NAT	(broadcast)
157.201.22.72/29	157.201.22.73	157.201.22.74 470t10ra.cit.byui.edu	157.201.22.75- 157.201.22.78	157.201.22.79

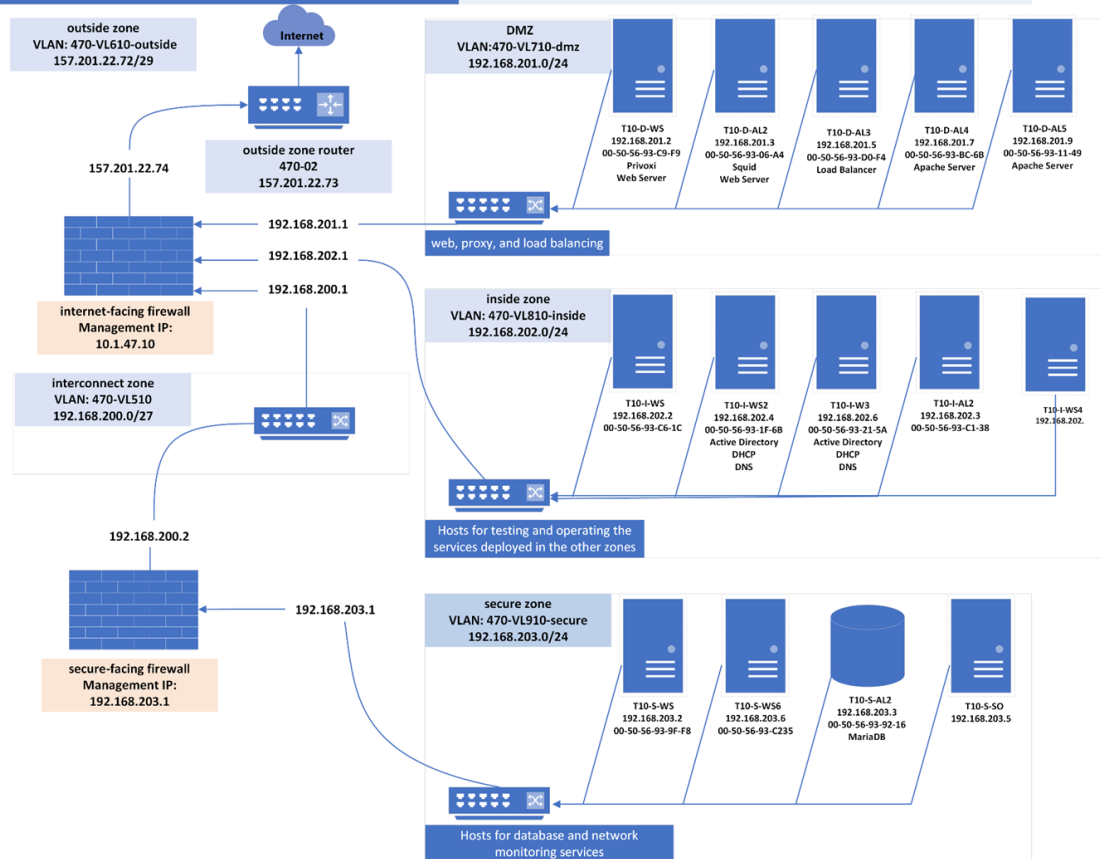
#### DNS addresses

Cloudflare  
1.1.1.1

Google  
8.8.8.8

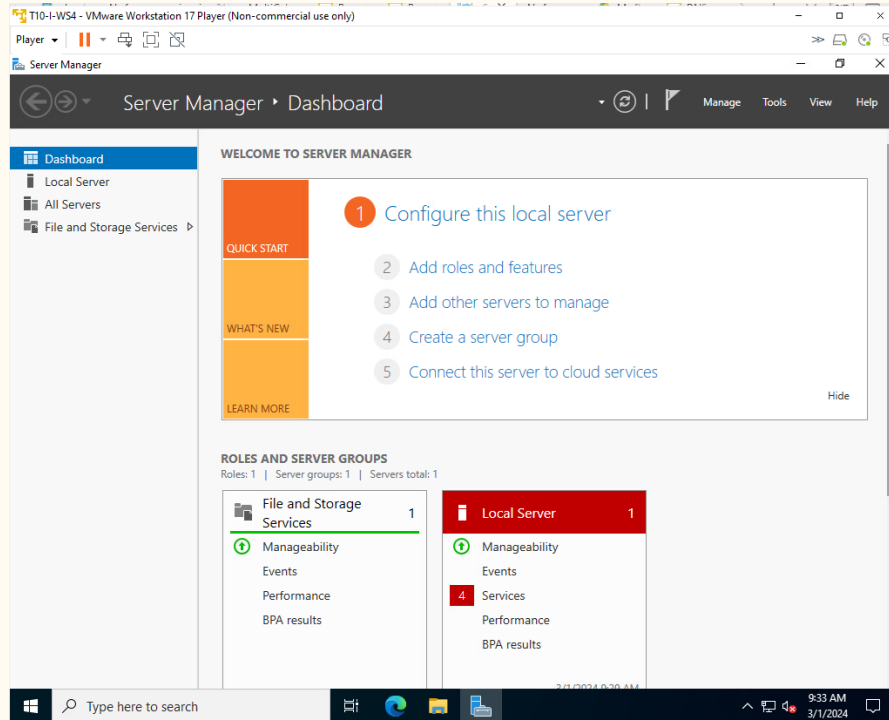
#### port numbers

#### application identifiers



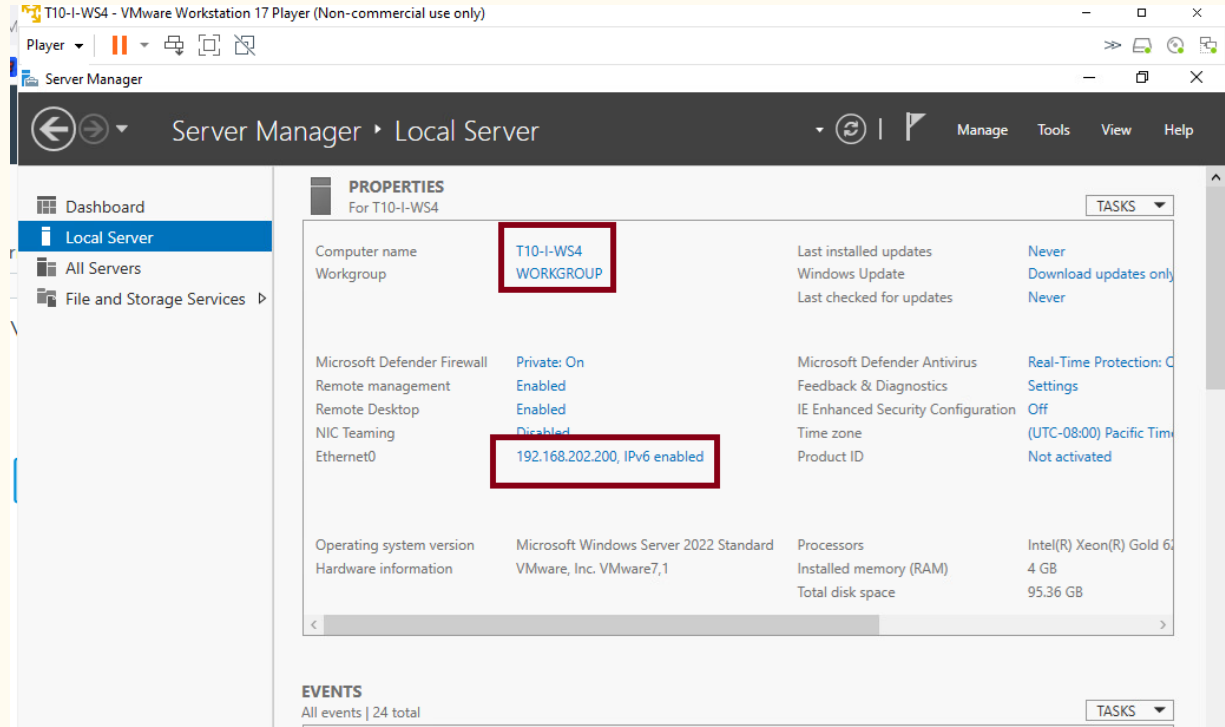
In order to configure the DHCP and DNS on our network I create a new testing server to install and configure DHCP and DNS.

The Windows server is in the intern zone since it has to provide ips to the DMZ and the secure zone.



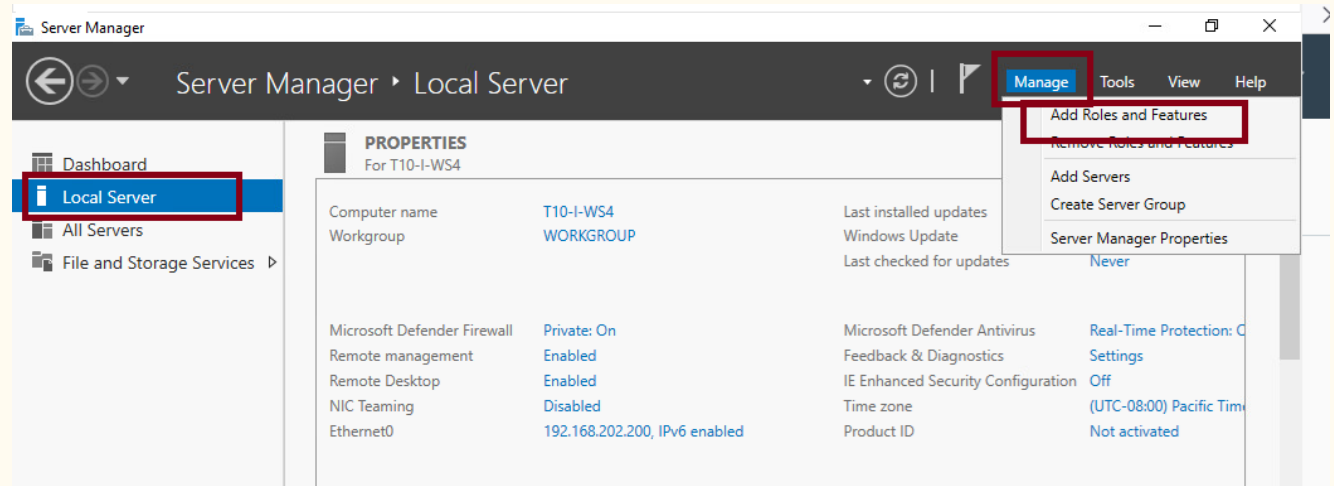
For this the Windows server is in the intern zone since it has to provide ips to the DMZ and the secure zone.

The name of the computer is T10-I-WS4 and have a static address of 192.168.202.200



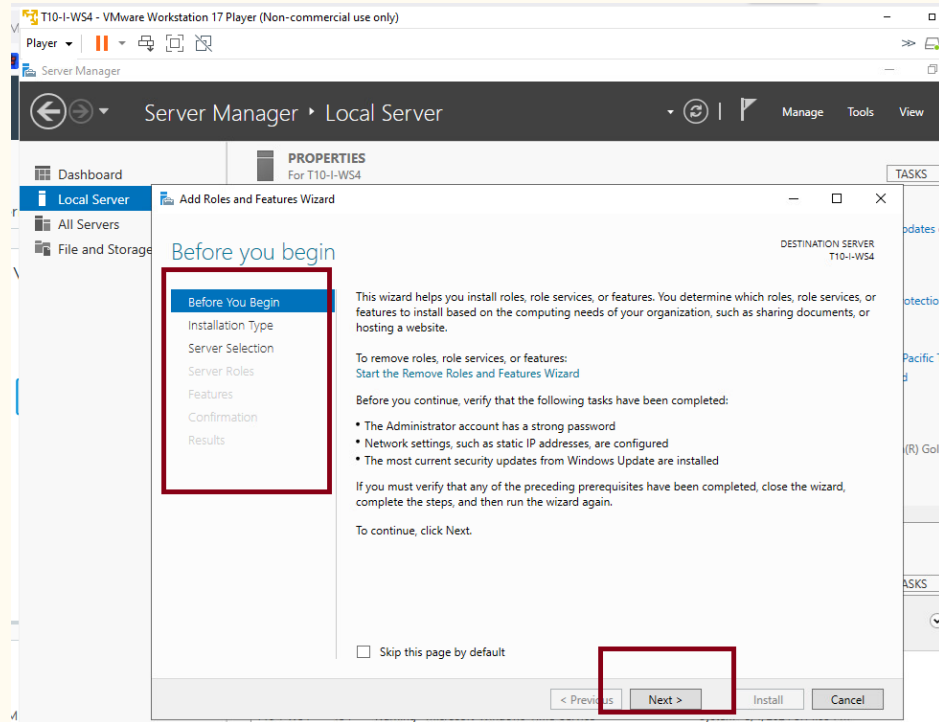
# Configuration of features.

Select local server, manage and add features. This is how those services are call in Windows.



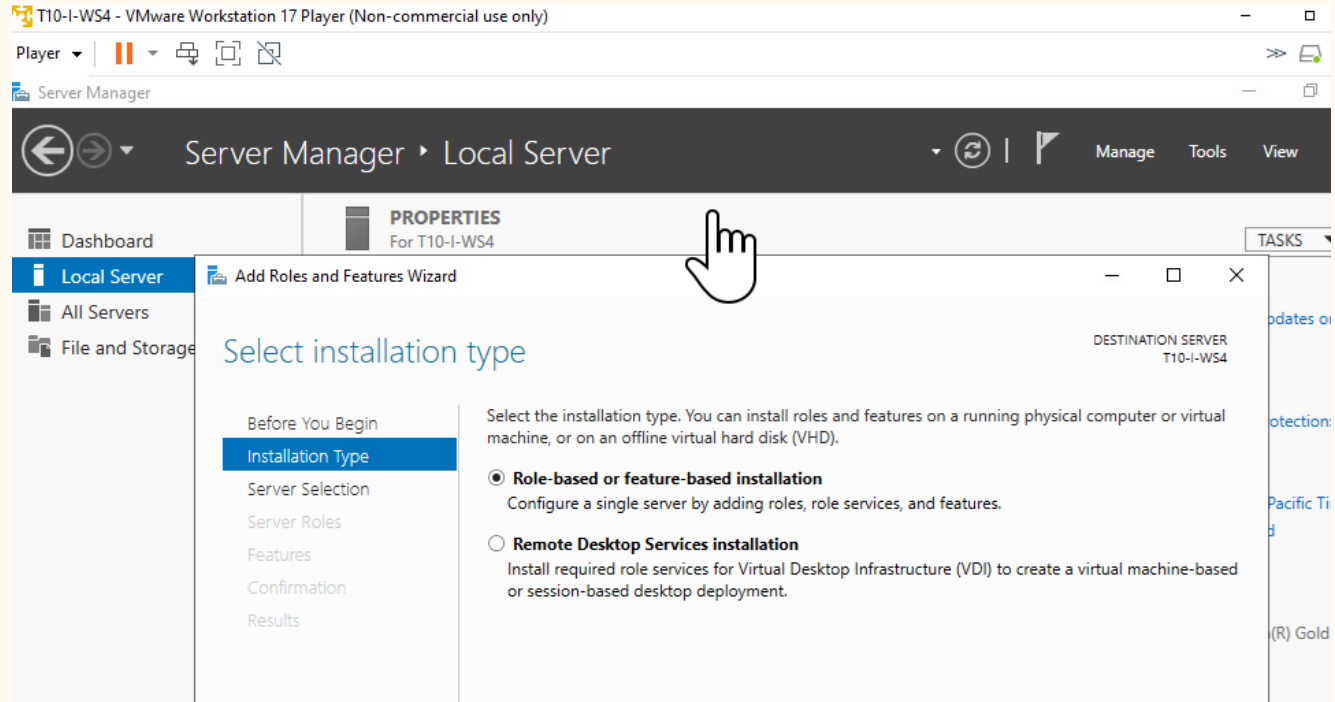
# Configuration of features.

The interface will guide you through the process of installation.



# Configuration of features.

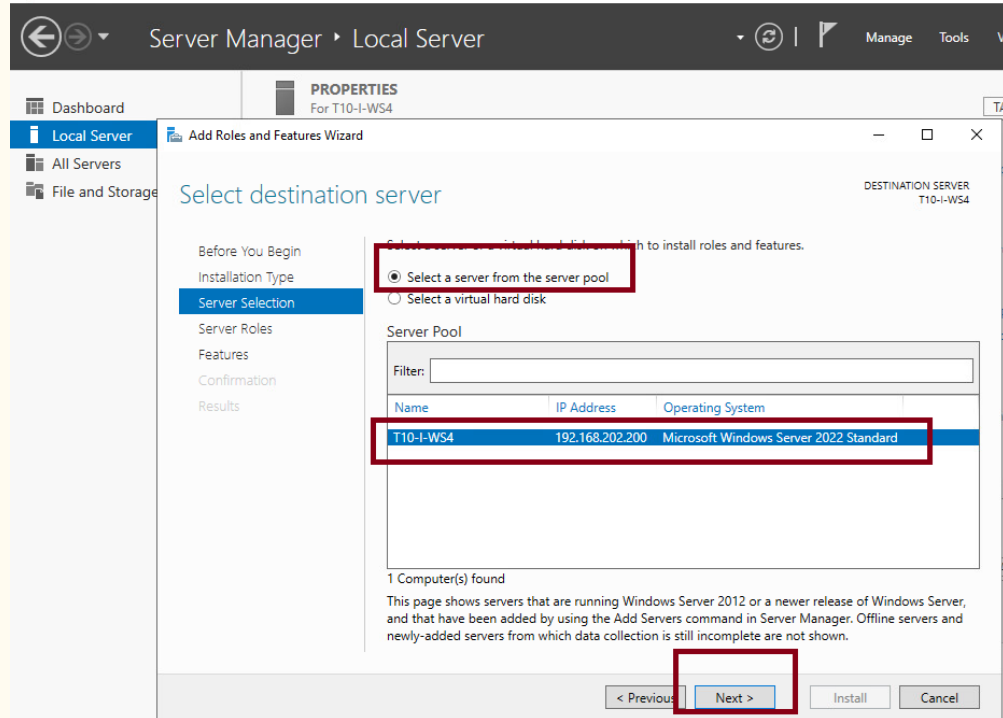
On Installation type select Role-based or featured-base installation.





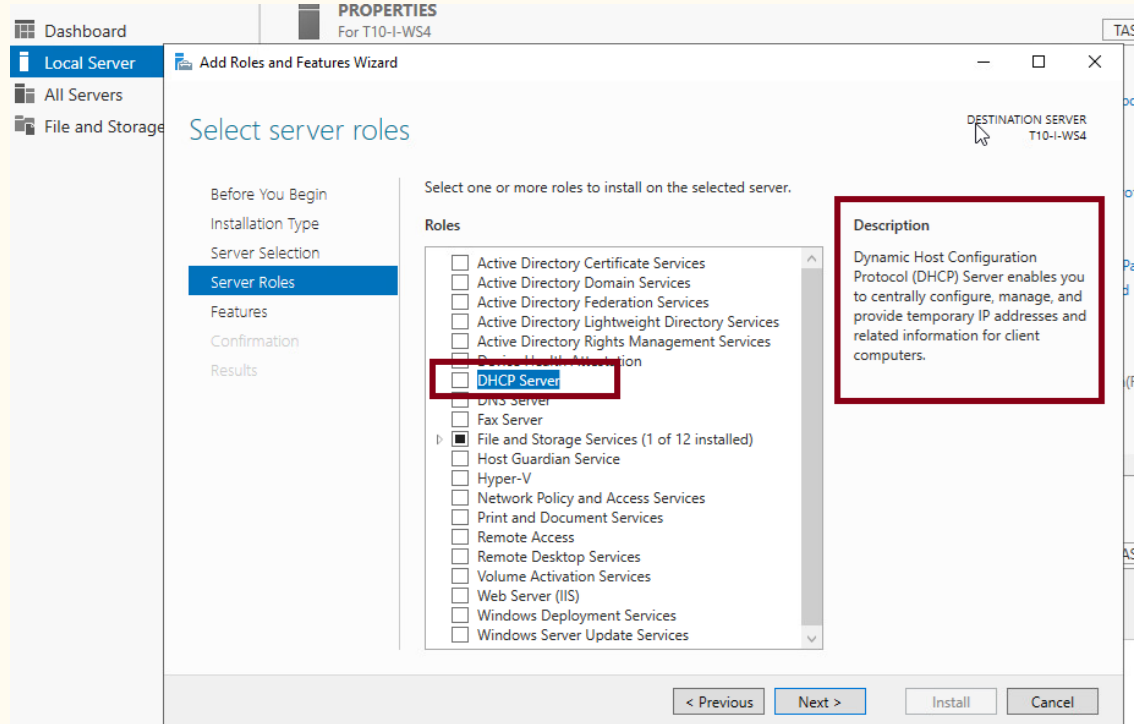
# Configuration of features.

On server selection  
select your server.



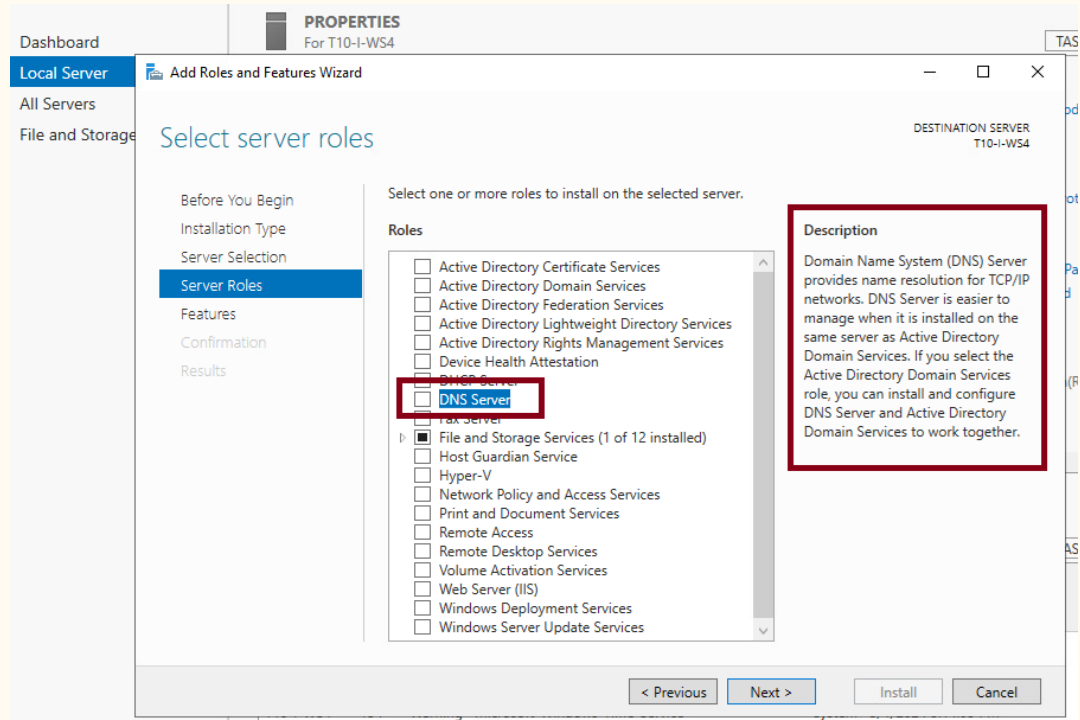
# Configuration of features.

On Server roles you must select DHCP.  
Read the description to know what is DHCP.



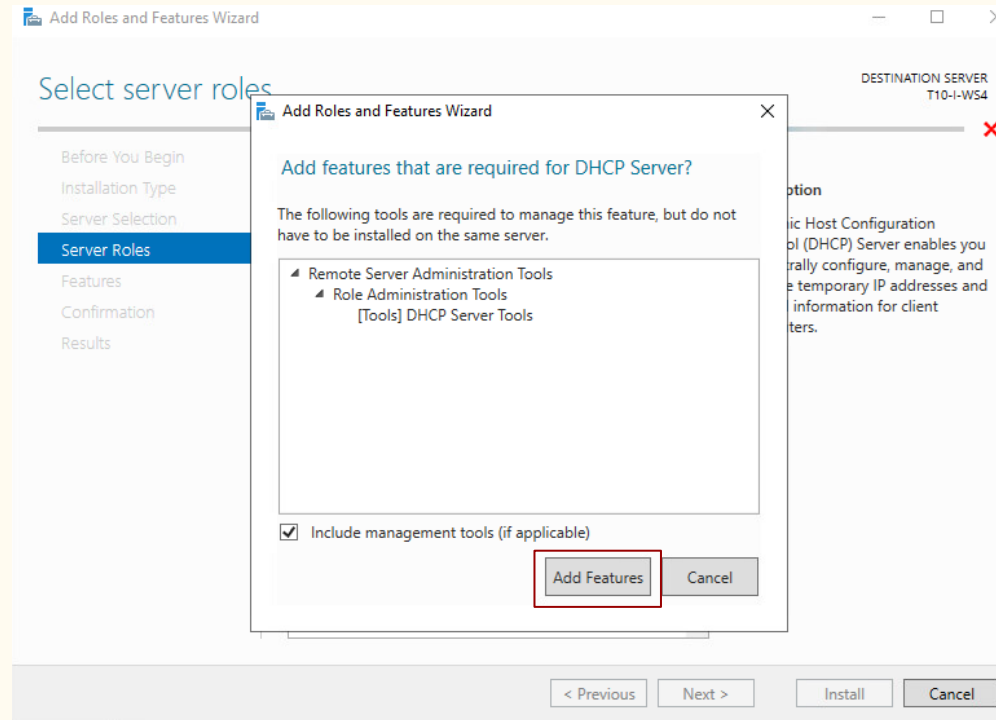
# Configuration of features.

Select also here  
DNS Server, and  
read the description.



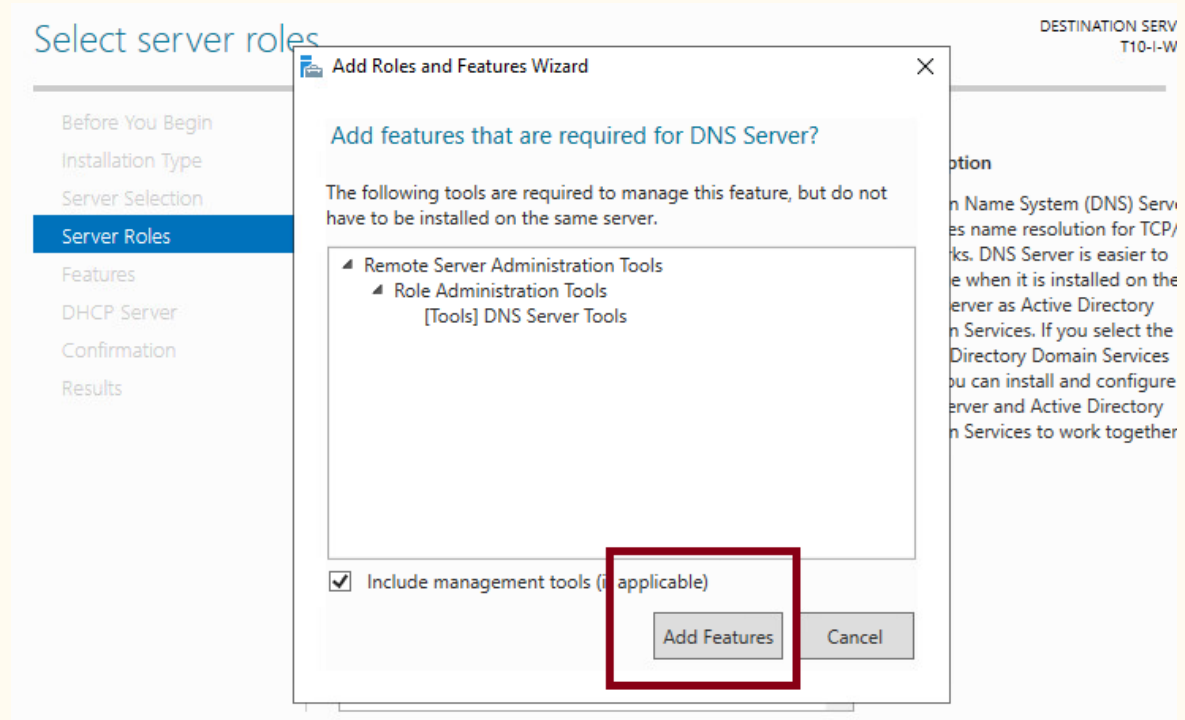
# Configuration of features.

In each case after select each role a window will open showing tools required to install together with each role. Select add features.



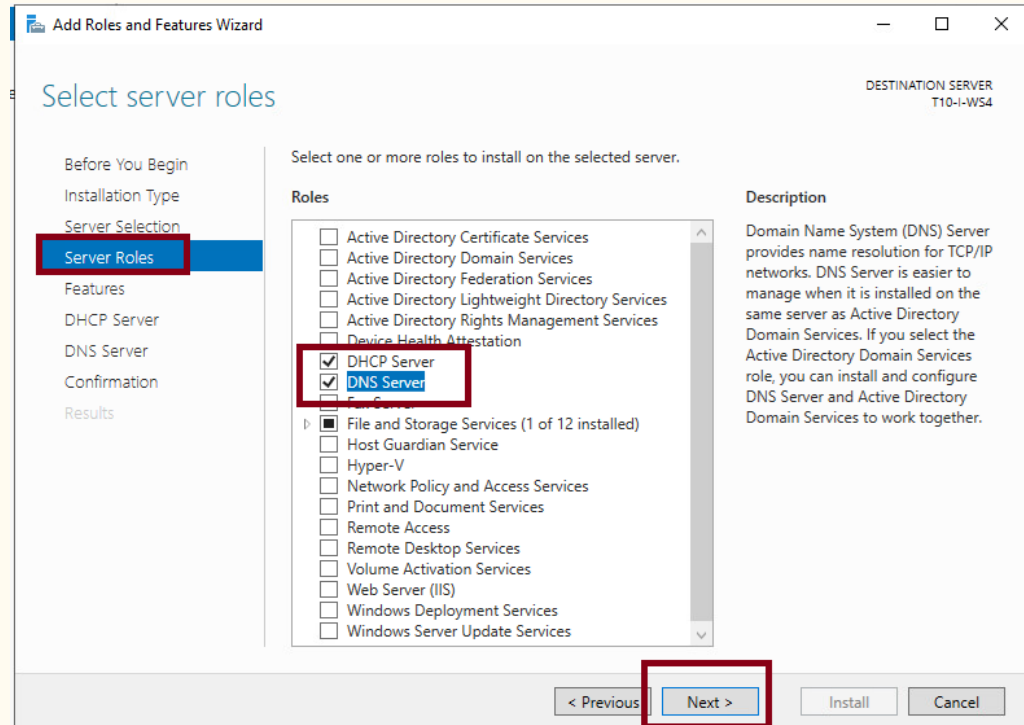
# Configuration of features.

Do the same with  
DNS role.



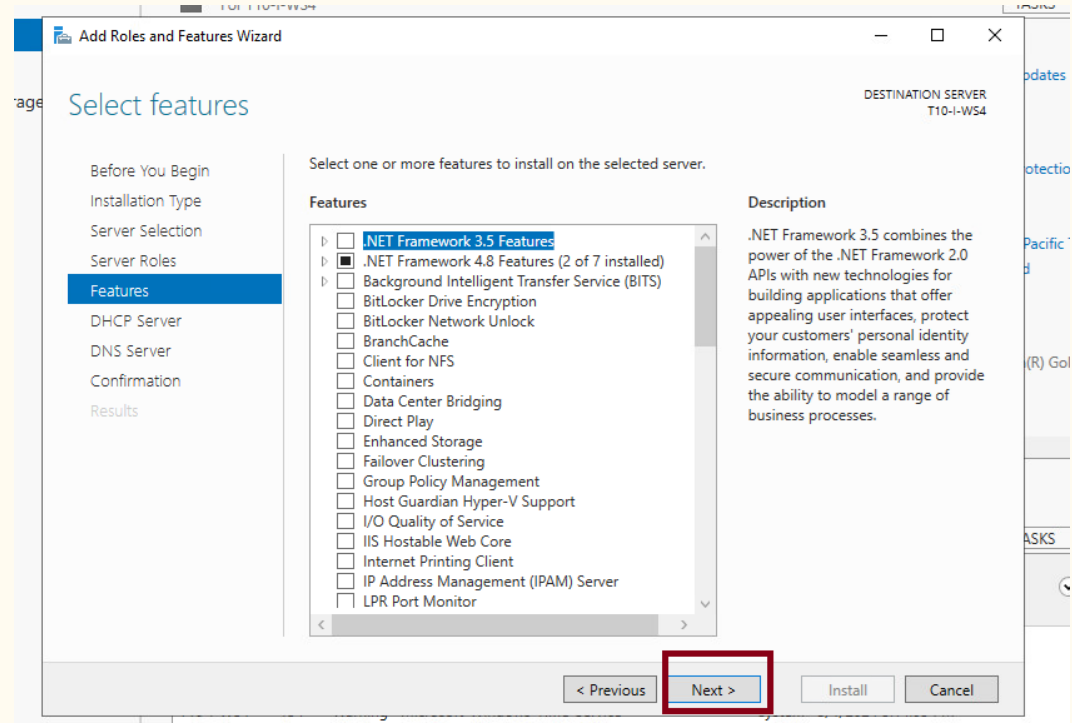
# Configuration of features.

Here is how should finish this step, with both features selected, click next.



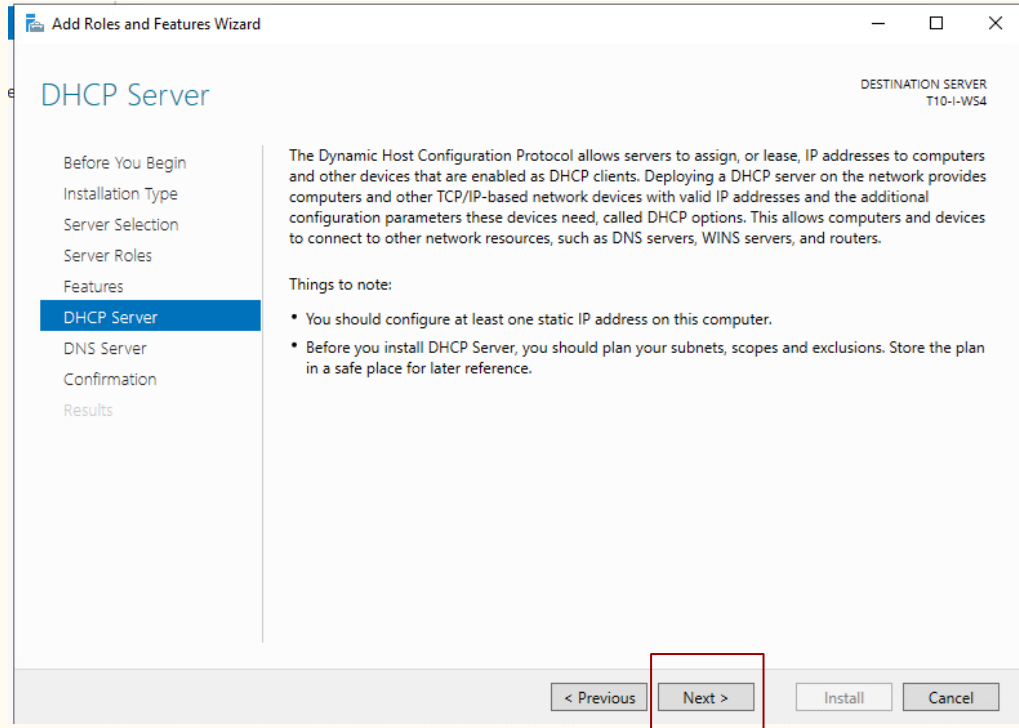
# Configuration of features.

On features click  
next.



# Configuration of features.

Select next after reading this description and notes.

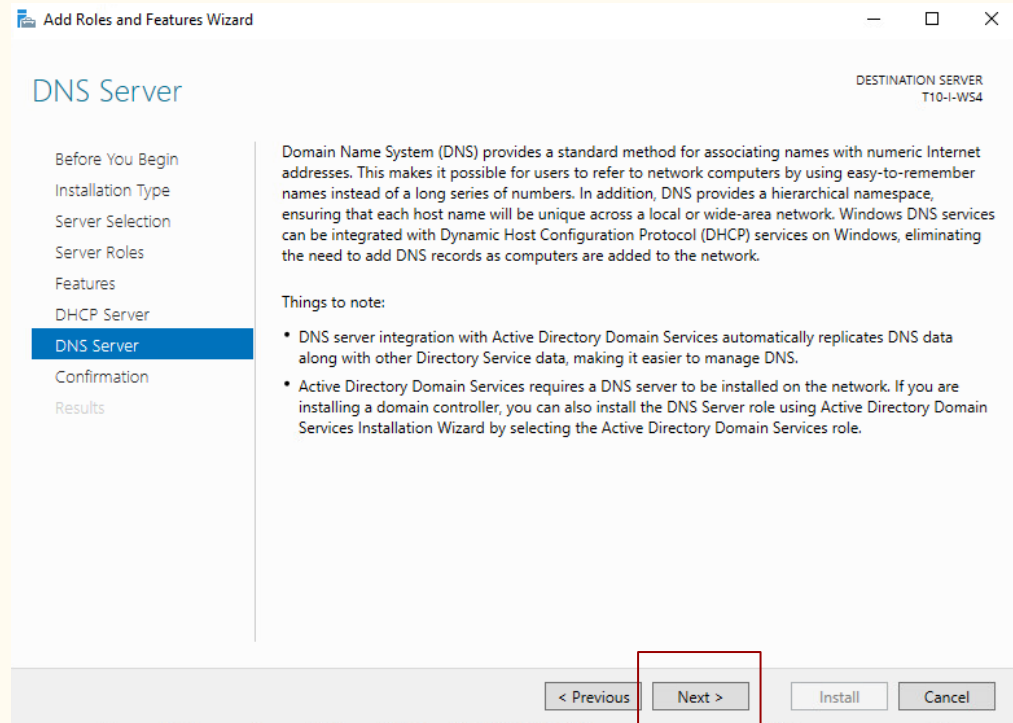




# Configuration of features.

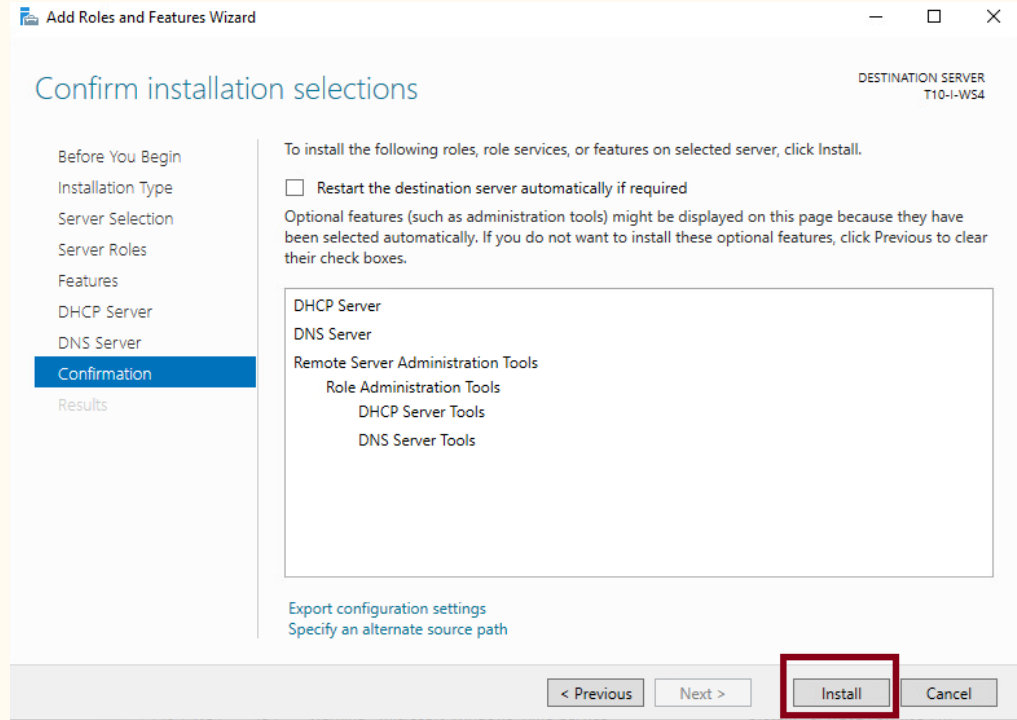
Select next after read the DNS information and things to note.

In this case we don't integrate with Active Directory for this demonstration. However the most secure choice will be integration with AD which give much more capabilities also.



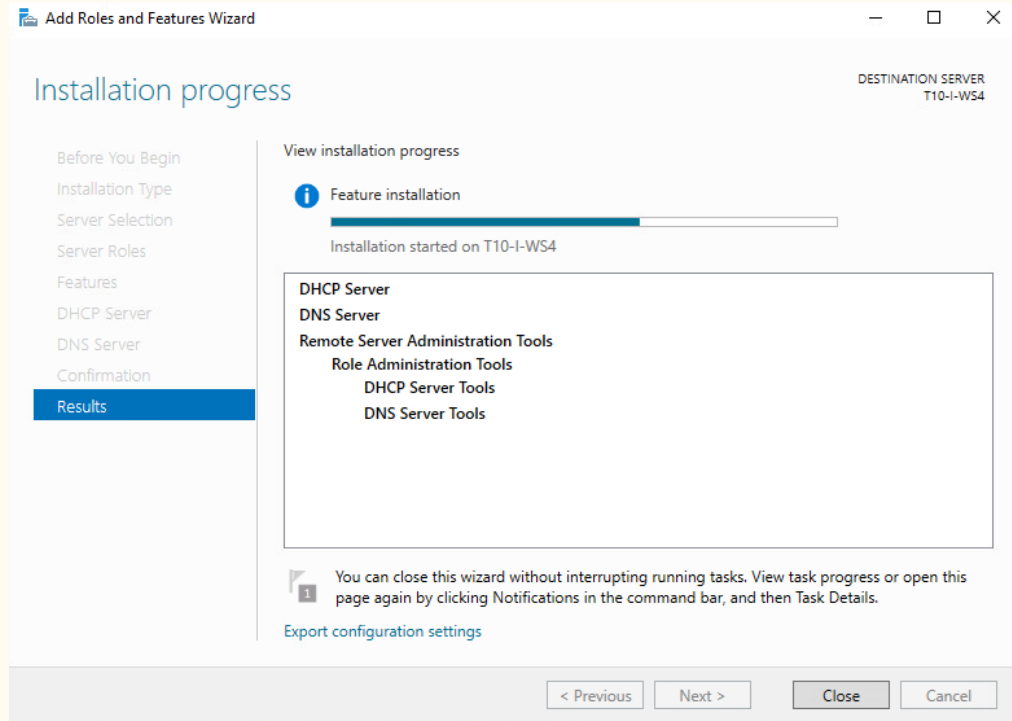
# Configuration of features.

The final confirmation shows a resume of the selected items to install. Select install to finish installation.



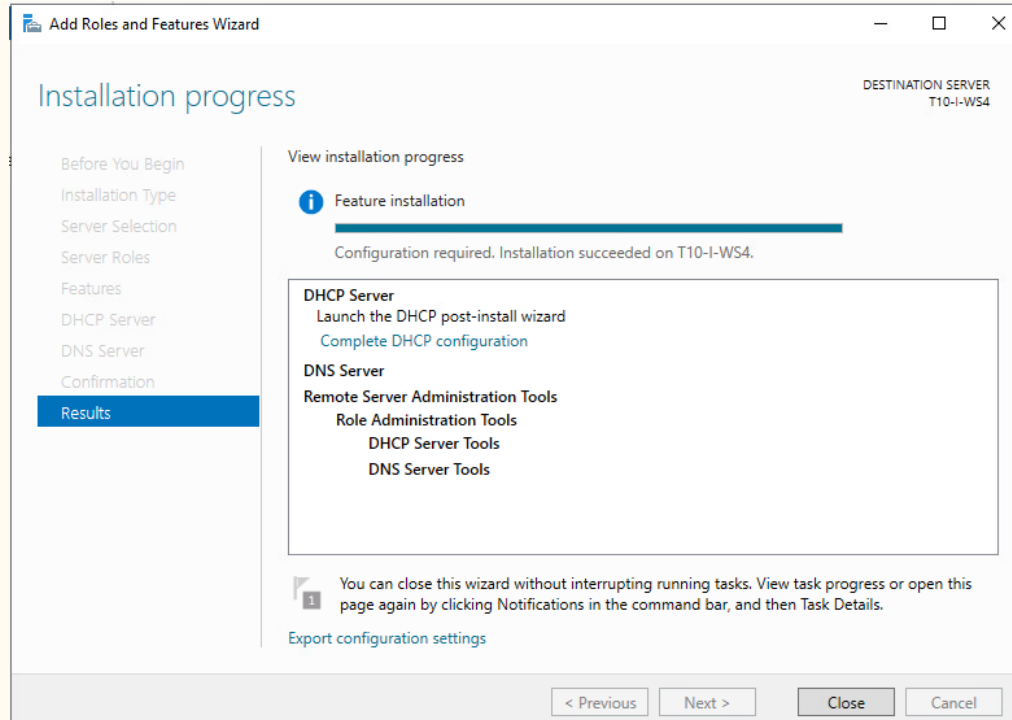
# Configuration of features.

The process takes some time while you will see this screen showing progression of the completion.



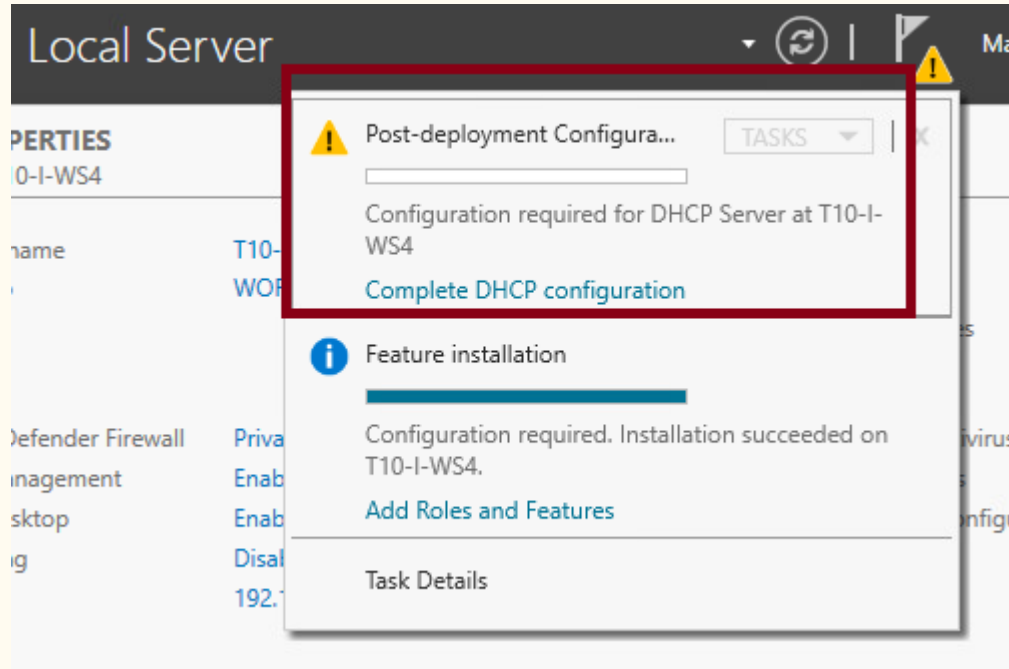
# Configuration of features.

This is the screen when the process is complete. Select close.



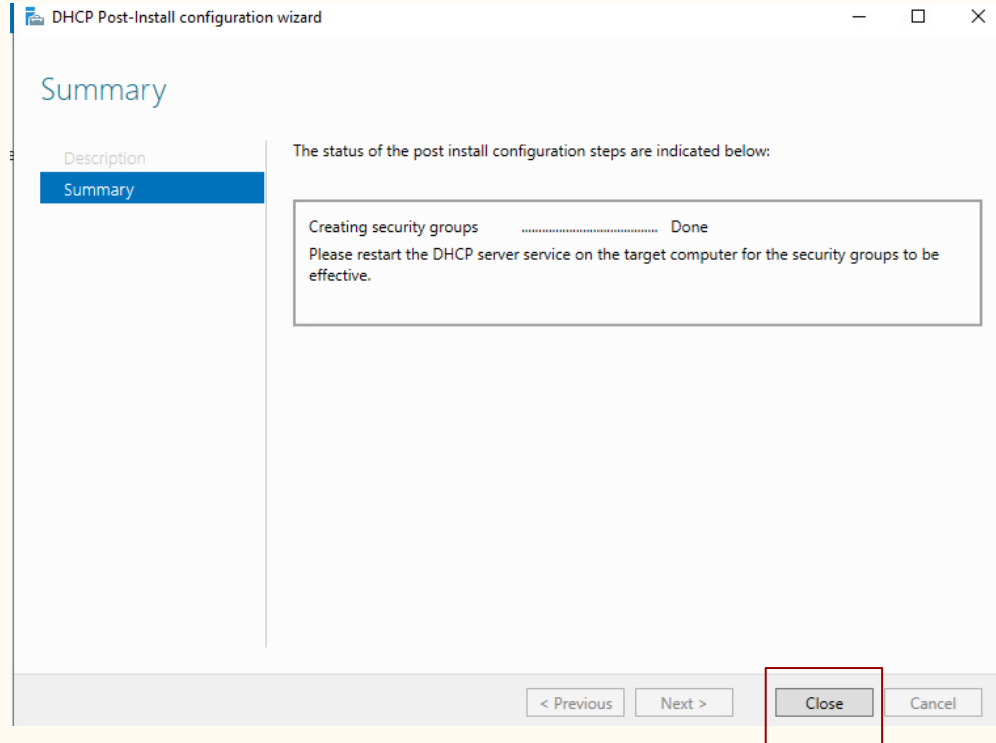
# Post-deployment configurations

You will see a warning asking for post deployment configurations. Click on Complete DHCP configuration.



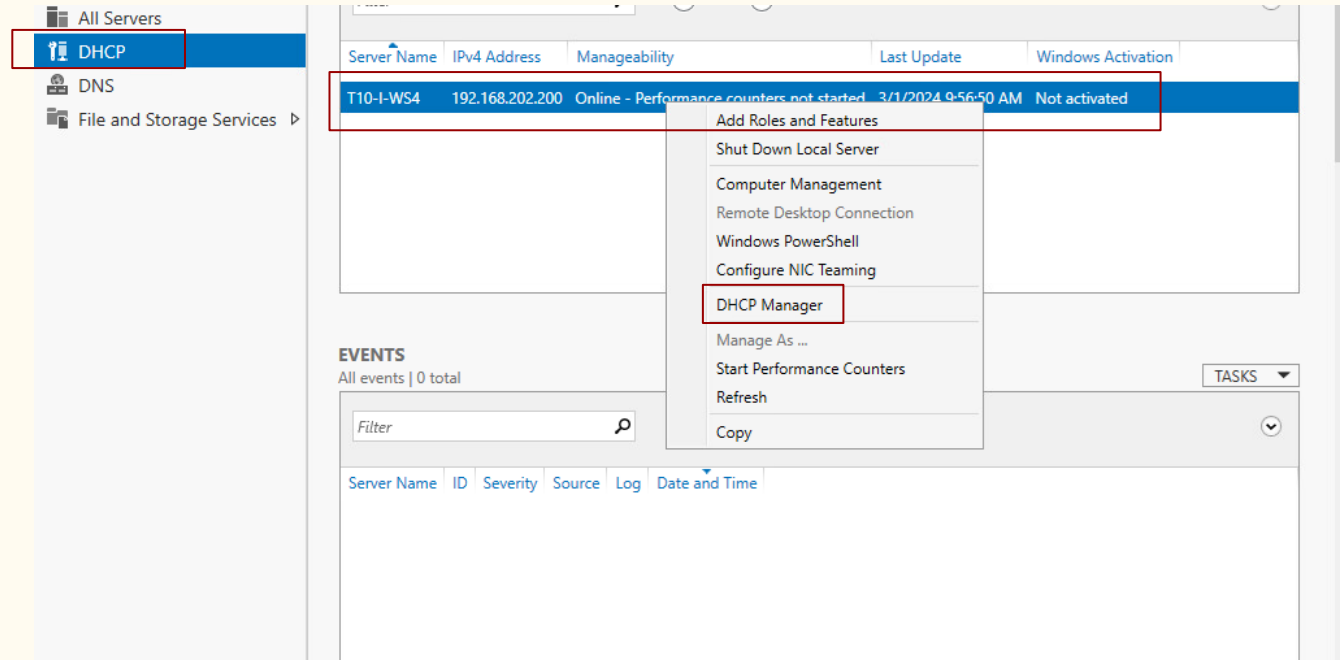
# Post-deployment configurations

This window will appear and it is not necessary any selection, wait until is done and select close.



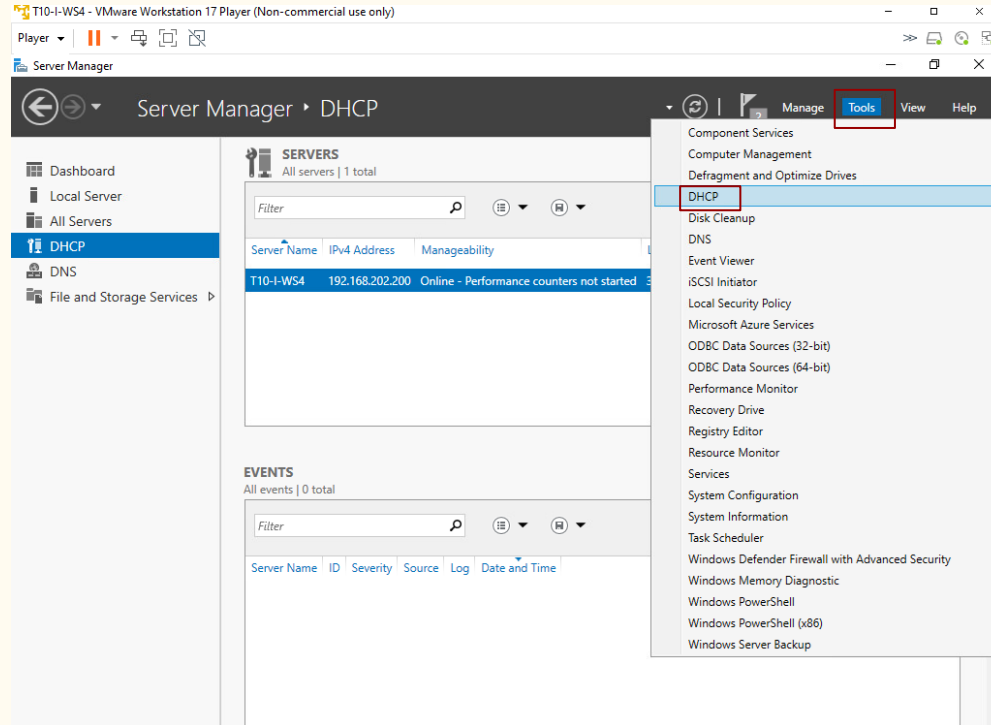
# DHCP configuration

There are 2 ways to go to DHCP manager. First you can click DHCP in the left side and in the server highlighted line right click in the mouse, and select DHCP Manager.



# DHCP configuration.

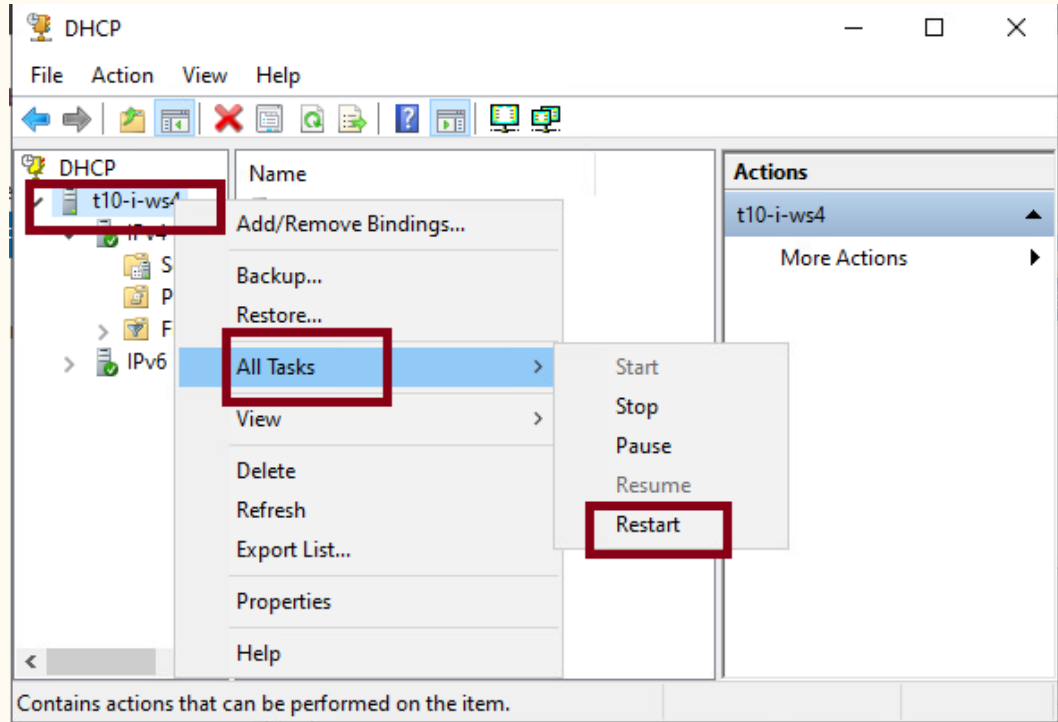
Second way to get to the same place is selecting from the top menu Tools, and then in the menu that opens, DHCP. Both ways works.





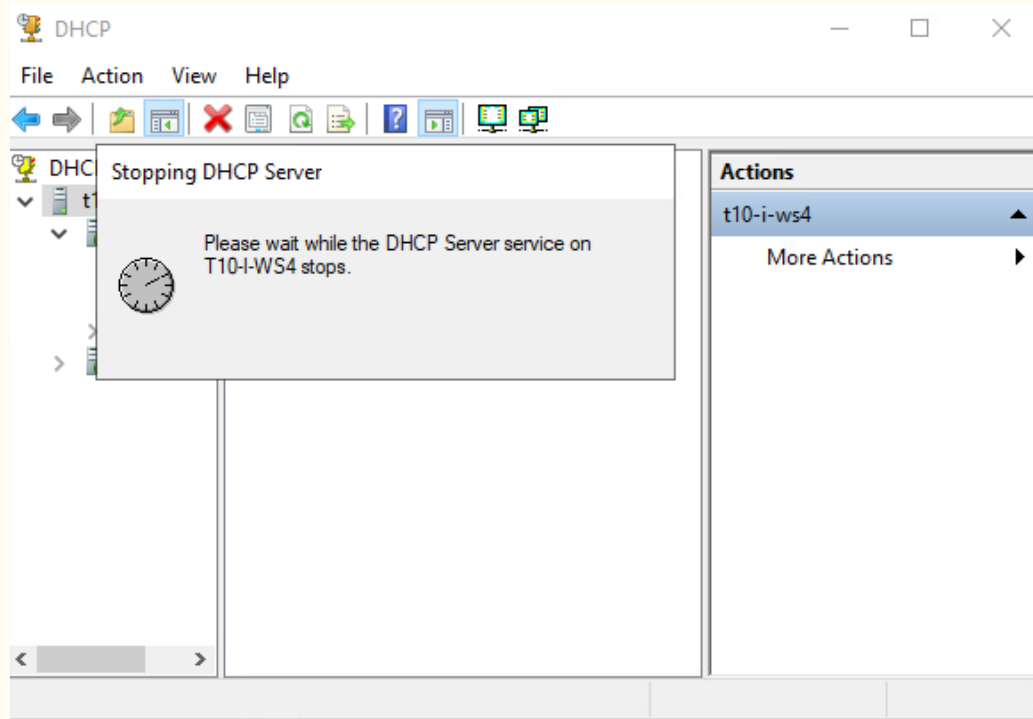
# DHCP configuration.

In the window that pop up, select the server icon, right click in the mouse and in all tasks, select restart.



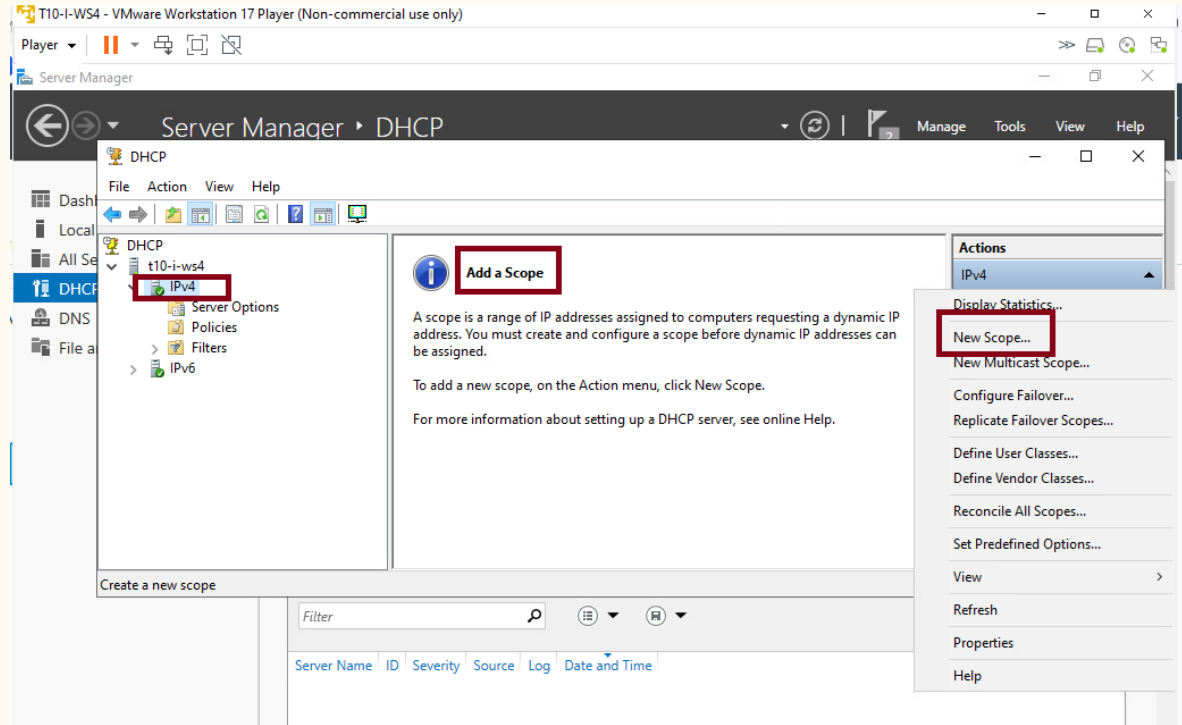
# DHCP configuration.

The server will  
restart to get all the  
last updates.



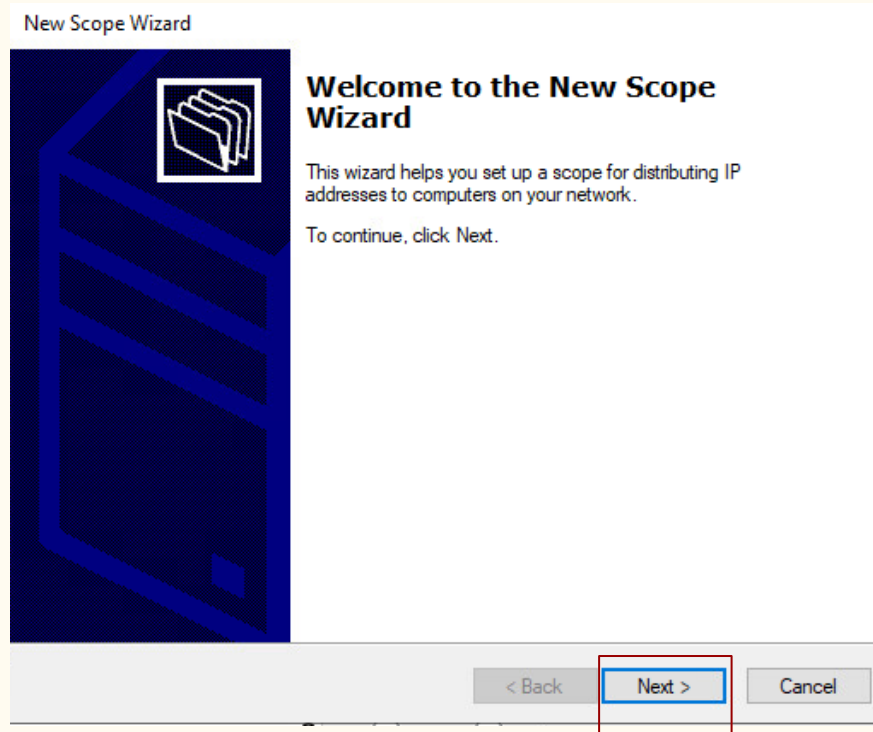
# DHCP configuration. Add scopes.

Under the server icon select IPv4 and new scope. A scope will create a range of address to offer to computers in an area of the network. Here we can also select information to give to the endpoints when they receive the IP from that range.



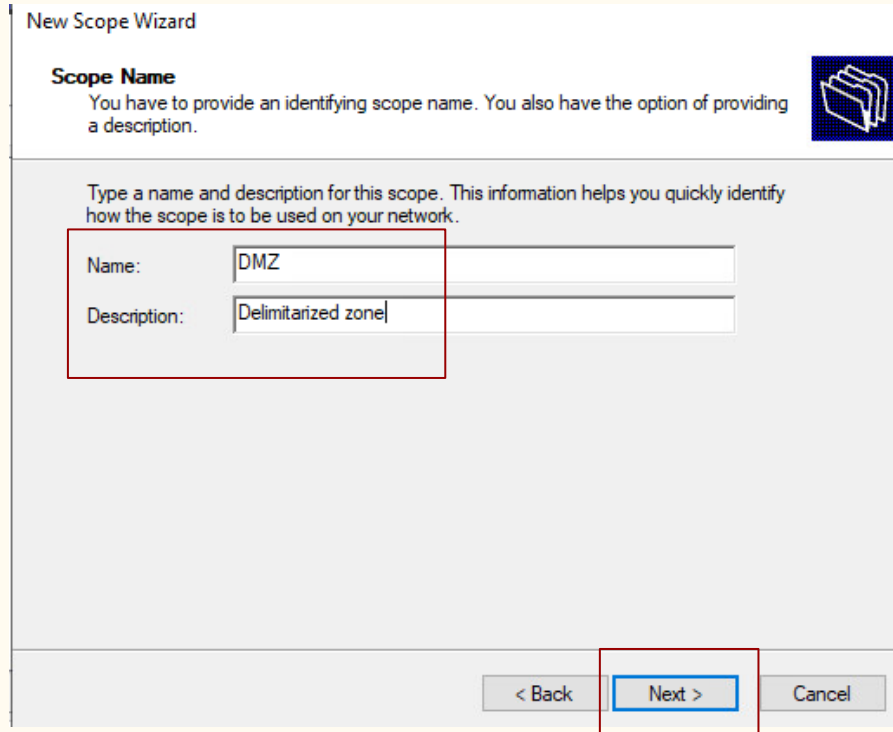
# DHCP configuration. Add scopes.

A new window pops up and will guide us on this process.  
Click next.



# DHCP configuration. Add scopes.

Here we start creating a scope for the DMZ. Put a name and a descriptor. Click next.



The image shows a 'New Scope Wizard' dialog box. It has a title bar 'New Scope Wizard' and a 'Scope Name' section with a folder icon. The text says: 'You have to provide an identifying scope name. You also have the option of providing a description.' Below this, it says: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' There are two input fields: 'Name:' with the value 'DMZ' and 'Description:' with the value 'Delimitarized zone'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

New Scope Wizard

**Scope Name**  
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: DMZ

Description: Delimitarized zone

< Back Next > Cancel

# DHCP configuration. Add scopes.

Add the range scope,  
and the subnet  
mask. Click next.

New Scope Wizard

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 201 . 2

End IP address: 192 . 168 . 201 . 100

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

# DHCP configuration. Add scopes.

In this occasion we don't add exclusions, just click next.

New Scope Wizard

**Add Exclusions and Delay**

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:  End IP address:

Excluded address range:

Subnet delay in milli second:

< Back **Next >** Cancel

# DHCP configuration. Add scopes.

We can configure the duration of the lease here. We can leave this with default values. Click next.

New Scope Wizard

**Lease Duration**  
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

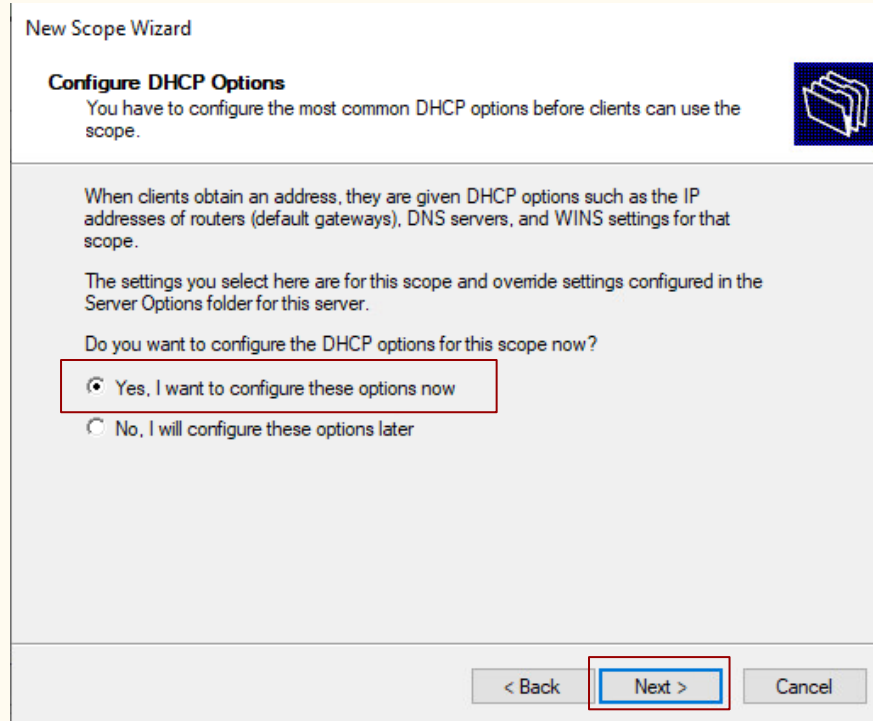
Days:	Hours:	Minutes:
1	0	0

< Back   **Next >**   Cancel



# DHCP configuration. Add scopes.

By choosing  
configure options we  
can configure extra  
information we give  
the client with each  
ip leased. Click next.



The image shows a screenshot of the 'New Scope Wizard' window in Windows Server. The title bar says 'New Scope Wizard'. The main heading is 'Configure DHCP Options'. Below it, a message states: 'You have to configure the most common DHCP options before clients can use the scope.' To the right of this message is a blue icon of a folder with a document. The main content area explains that DHCP options like IP addresses of routers, DNS servers, and WINS settings are given to clients. It also notes that settings selected here override those in the 'Server Options' folder. A question is posed: 'Do you want to configure the DHCP options for this scope now?'. There are two radio button options: 'Yes, I want to configure these options now' (which is selected and highlighted with a red rectangle) and 'No, I will configure these options later'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red rectangle), and 'Cancel'.

New Scope Wizard

**Configure DHCP Options**

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back   Next >   Cancel

# DHCP configuration. Add scopes.

Here we configure a default gateway for the zone. Click add and next.

New Scope Wizard

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:  
192 . 168 . 201 . 1

Add

Remove

Up

Down

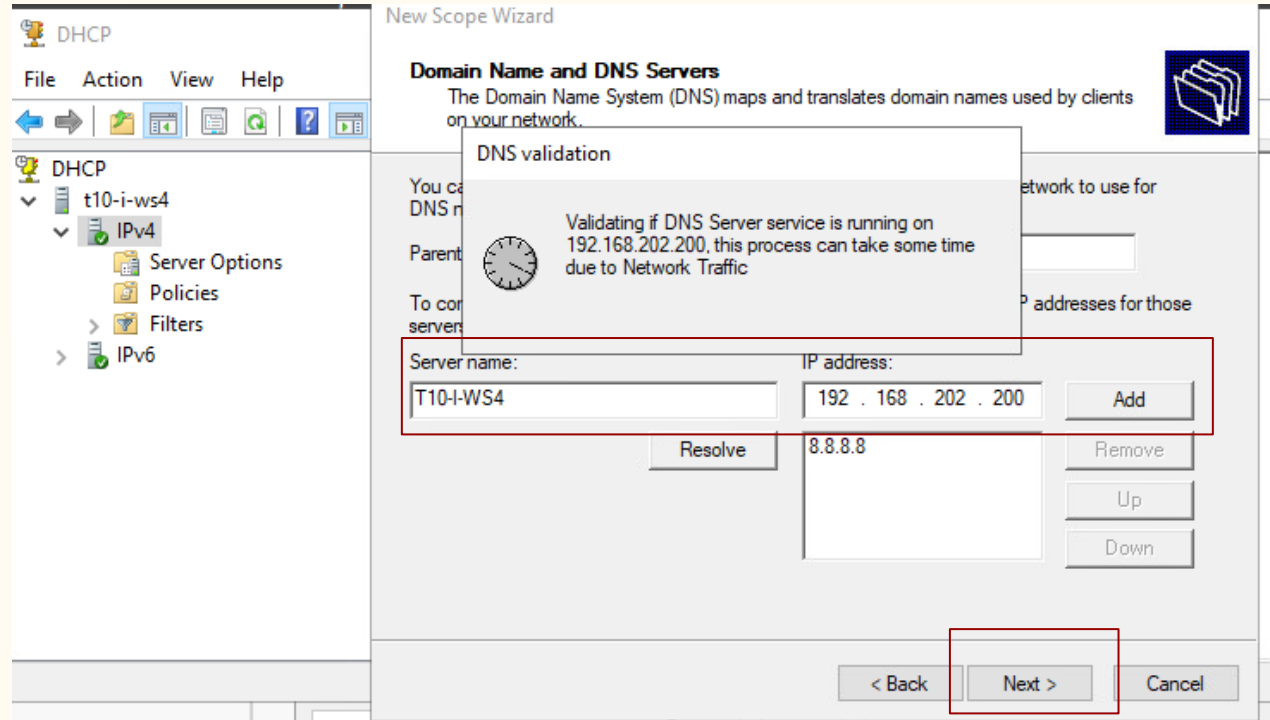
< Back

Next >

Cancel

# DHCP configuration. Add scopes.

On domain name write first the server name and ip address of your server, and select add. It will take a while to check if DNS is running on your server.



# DHCP configuration. Add scopes.

After validation you  
can select next.

New Scope Wizard

**Domain Name and DNS Servers**  
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

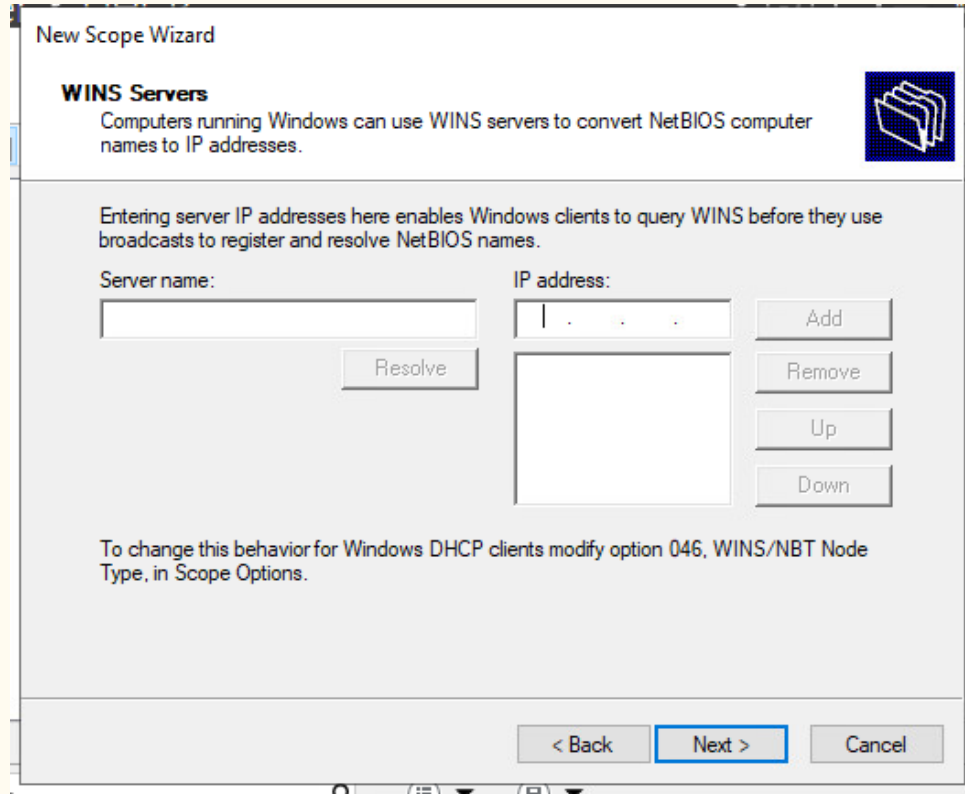
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text" value="T10-I-WS4"/>	<input type="text" value="1 . . ."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<div>8.8.8.8 192.168.202.200</div>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

< Back   **Next >**   Cancel

# DHCP configuration. Add scopes.

In this case we will not configure WINS servers.



The screenshot shows the 'New Scope Wizard' window, specifically the 'WINS Servers' step. The window title is 'New Scope Wizard'. Below the title bar, there is a section header 'WINS Servers' followed by a description: 'Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.' To the right of this text is a small icon of a folder with a document. Below the description, there is a paragraph explaining the purpose: 'Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.' The main area contains two input fields: 'Server name:' and 'IP address:'. The 'Server name' field has a 'Resolve' button next to it. The 'IP address' field has an 'Add' button next to it. Below the 'IP address' field is a list box, and to its right are 'Remove', 'Up', and 'Down' buttons. At the bottom of the window, there is a note: 'To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.' The bottom of the window features three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Scope Wizard

**WINS Servers**  
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

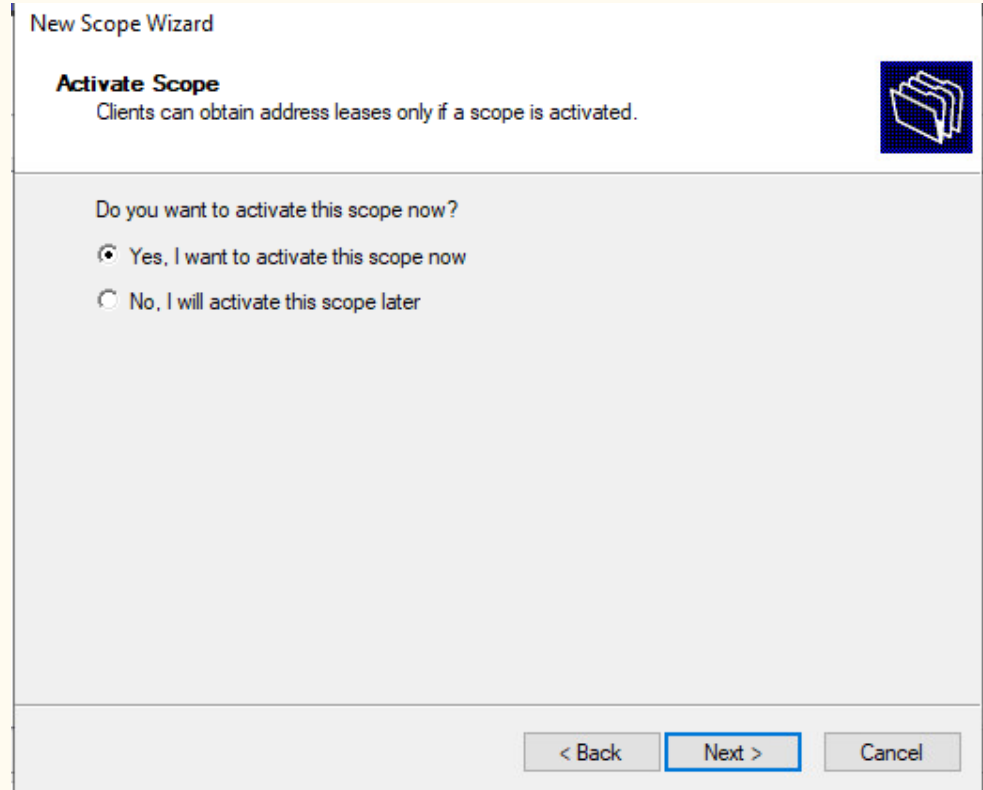
IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

< Back **Next >** Cancel

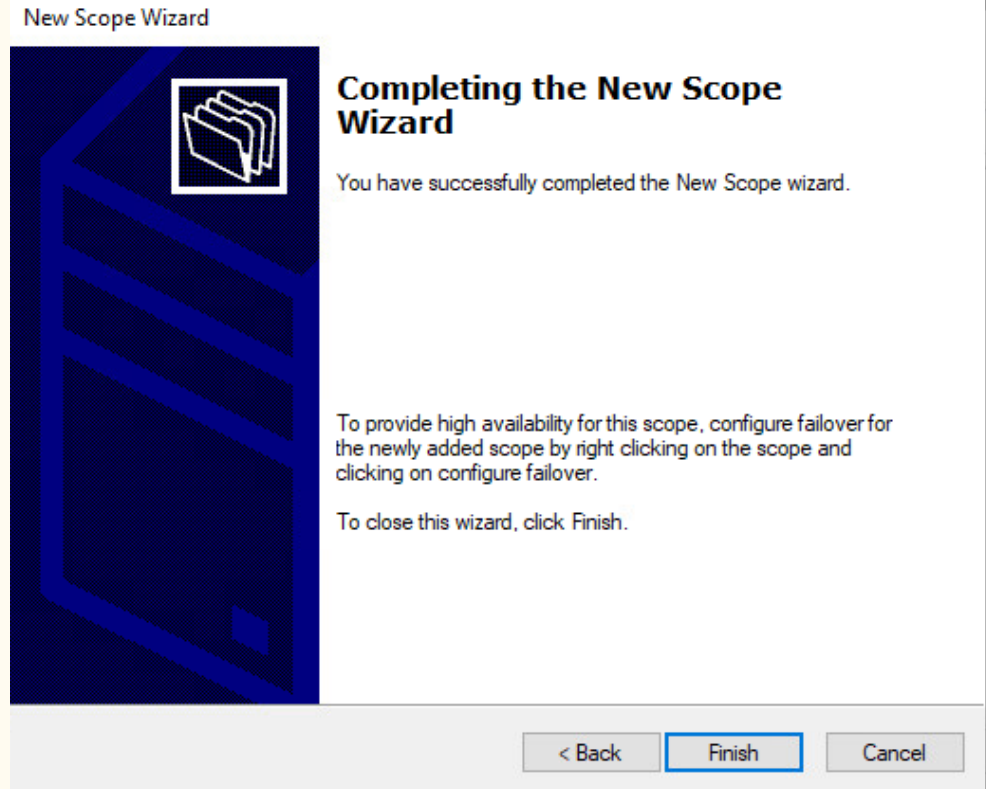
# DHCP configuration. Add scopes.

Here we can activate the scope and start to send ips and receive broadcast from new clients. Since we already had a domain in the network we decided to not activate this scope yet.



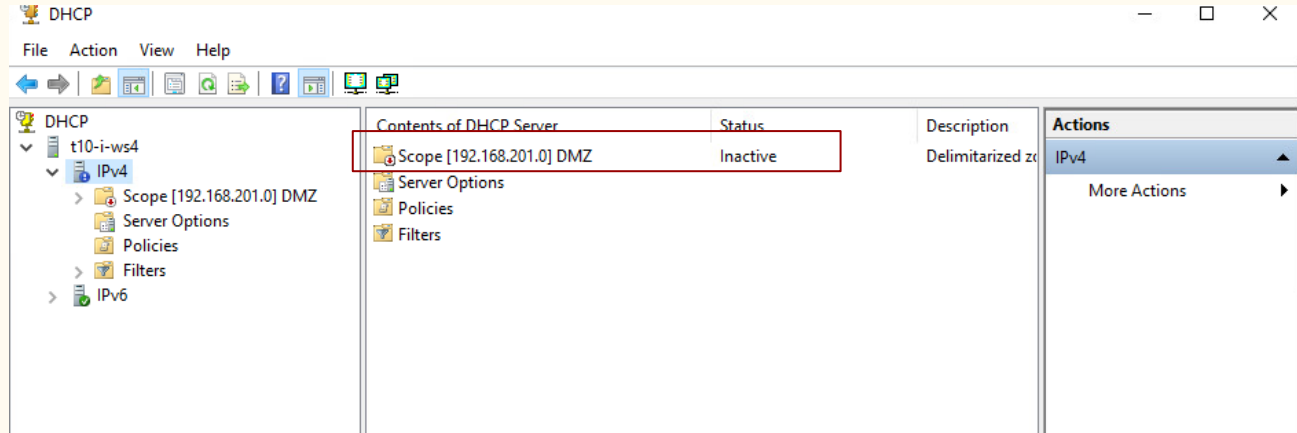
# DHCP configuration. Add scopes.

We now select finish to complete the configuration of our first scope for the DMZ.



# DHCP configuration. Add scopes.

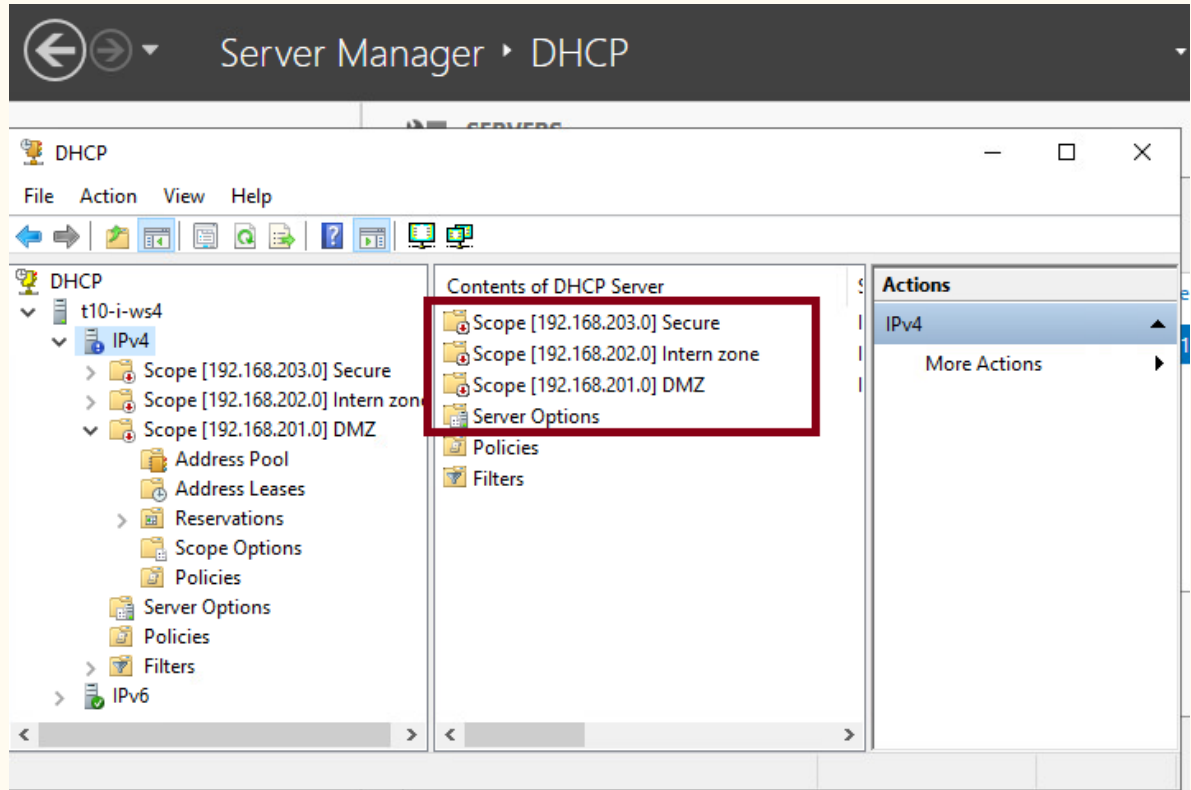
The first scope will appear on the interface. Paid attention to the red mark on the scope icon showing that is not active. We can activate the scope by right clicking in the scope and choose activate.





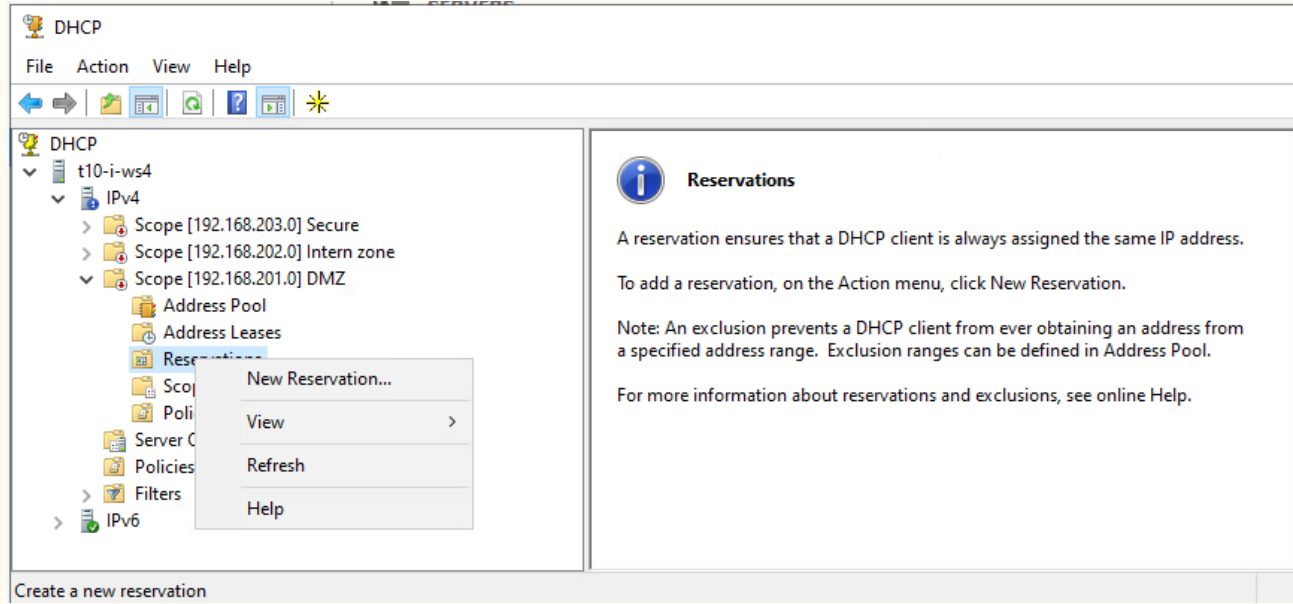
# DHCP configuration. Add scopes.

The same process should be repeated for each scope to mimic the organization of our network.



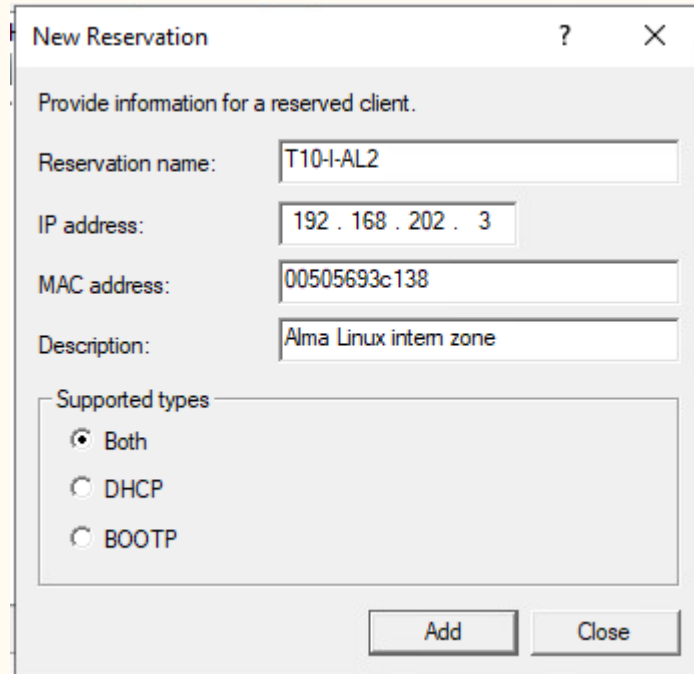
# DHCP configuration. Add sticky addresses for our servers.

It is not secure and impractical that our servers lease different ips . To solve that we assign specific addresses to those machines. We link machines MAC identifications with fixed ips when we create reservations. On each scope we open the reservations tab and select new reservation to start.



# DHCP configuration. Add sticky addresses for our servers.

You will need the name, ip address to reserve, and the MAC address for each machine. Add a description and leave both selected. Finish with add. A new window will open where you can add more reservations for your entire scope.



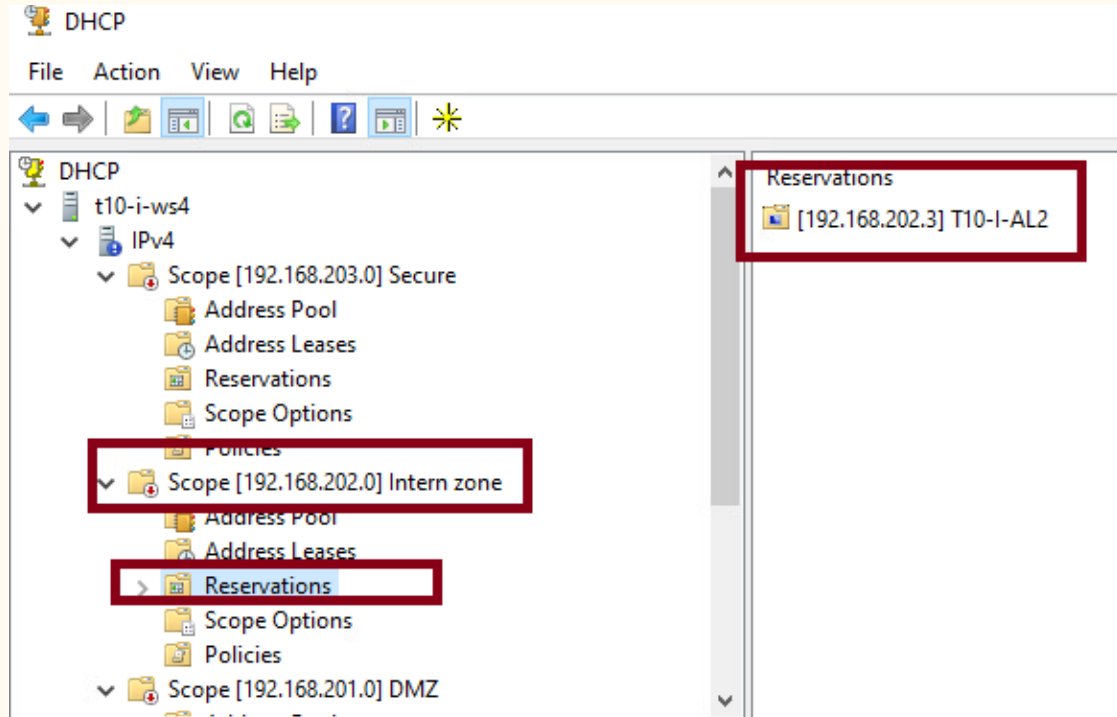
The screenshot shows a 'New Reservation' dialog box with the following fields and options:

- Reservation name:** T10-I-AL2
- IP address:** 192 . 168 . 202 . 3
- MAC address:** 00505693c138
- Description:** Alma Linux intern zone
- Supported types:**
  - ☒ Both
  - ☐ DHCP
  - ☐ BOOTP

At the bottom right, there are two buttons: 'Add' and 'Close'.

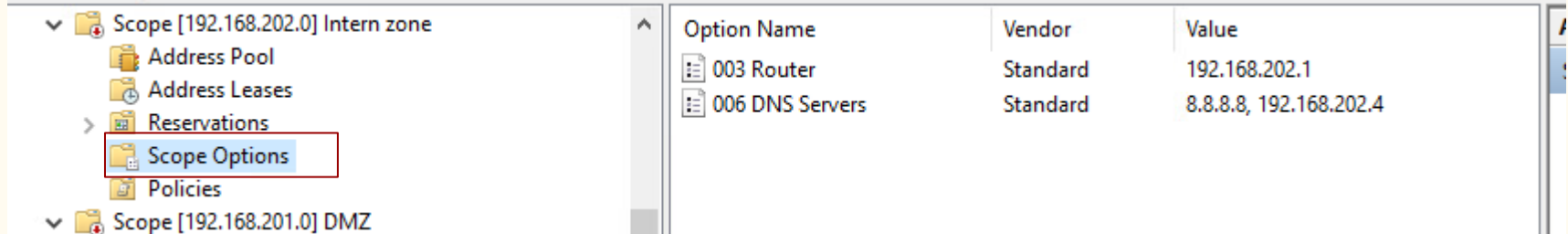
# DHCP configuration. Add sticky addresses for our servers.

When finish, close the window, and you will see the new reservations under your scope. Repeat the same operation for each server on your network.



# DHCP configuration. Scope options.

You already configure a DNS and default gateway for each scope. But you can add much more information than that by click on scope options and add different preset parameters. You can also change or update this information.

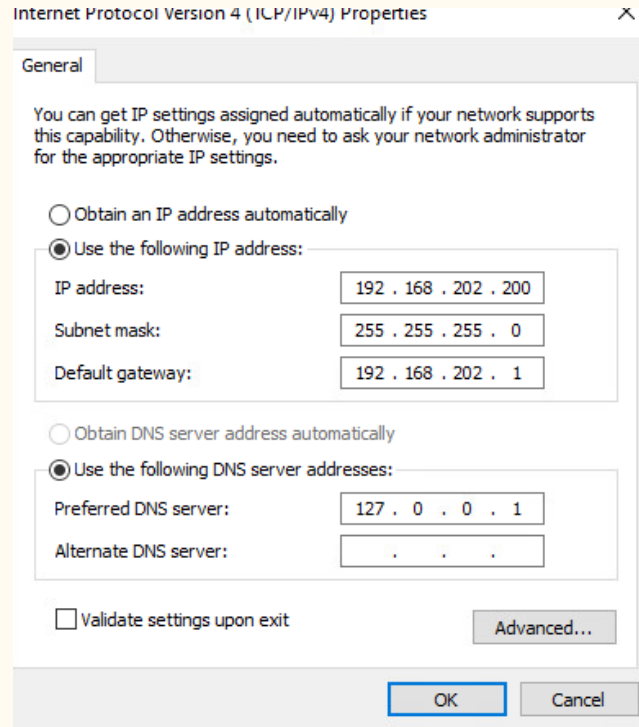


The screenshot shows the DHCP console interface. On the left, a tree view displays the hierarchy: 'Scope [192.168.202.0] Intern zone' is expanded, showing sub-items: 'Address Pool', 'Address Leases', 'Reservations', 'Scope Options' (highlighted with a red rectangle), and 'Policies'. Below it is 'Scope [192.168.201.0] DMZ'. On the right, a table displays the configuration for the selected 'Scope Options'.

Option Name	Vendor	Value
003 Router	Standard	192.168.202.1
006 DNS Servers	Standard	8.8.8.8, 192.168.202.4

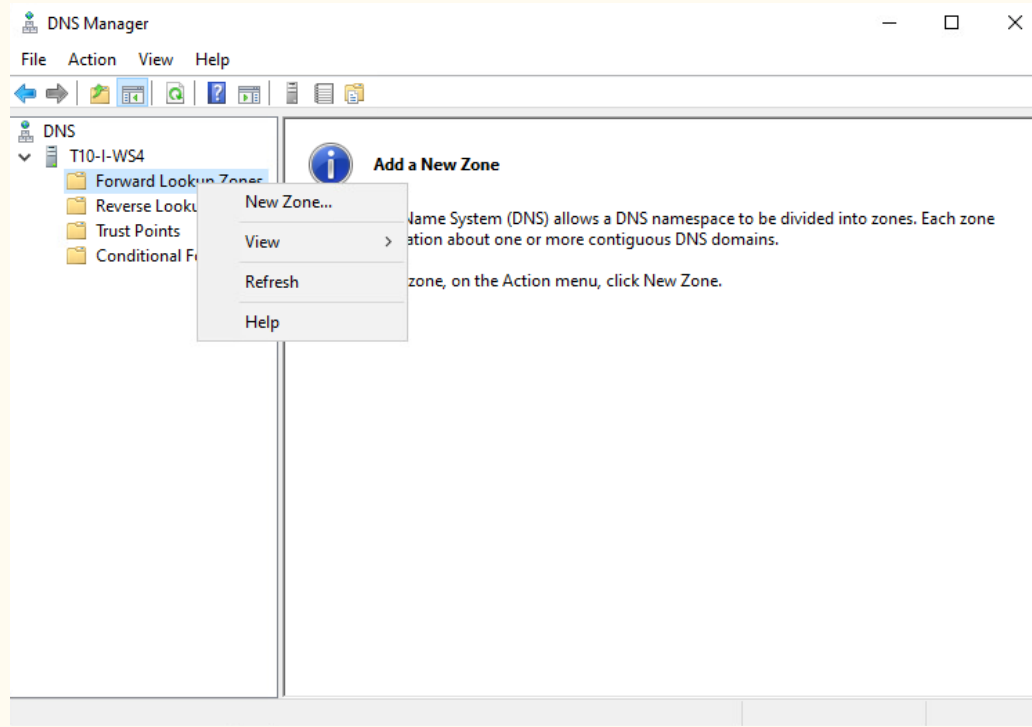
# DNS Configuration on DNS server.

Your DNS is running and working properly, then you can configure the server to receive dns services from that role installed. Change the preferred DNS server to point to himself by selecting 127.0.0.1 as preferred DNS.



# DNS configurations.

To resolve addresses in our network DNS needs to create register in his database based on DHCP leases or update information in his database. For that purpose first we create a forward lookup zone. Open the DNS manager in the same way you open the DHCP service manager. Select forward lookup zone and new zone.



# DNS configurations.

This interface will guide us along the configuration process.





# DNS configurations.

Select Primary zone  
in the first window  
and click next.

New Zone Wizard

**Zone Type**  
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

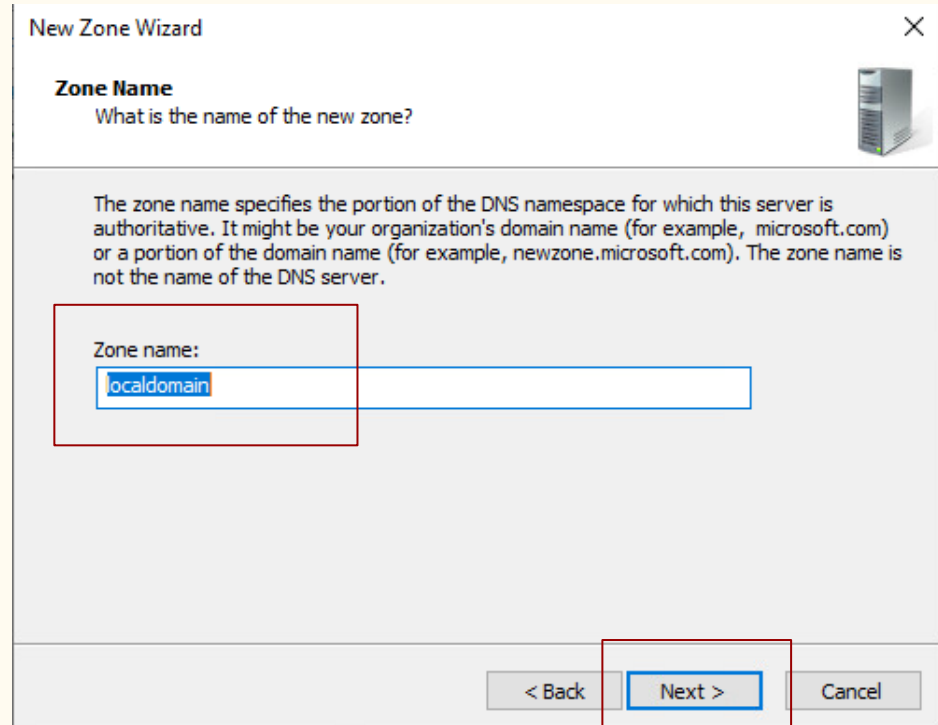
- ☒ **Primary zone**  
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**  
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**  
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☐ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back   **Next >**   Cancel

# DNS configurations.

If we have an Active Directory, we will add the domain name here. Since this is a standalone system we add localdomain. Select next.



The image shows a Windows 'New Zone Wizard' dialog box. The title bar says 'New Zone Wizard' with a close button. The main heading is 'Zone Name' with a sub-question 'What is the name of the new zone?'. To the right is a server icon. Below this is a text box explaining: '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.' Below the explanation is a text input field labeled 'Zone name:' containing the text 'localdomain'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.

New Zone Wizard

**Zone Name**  
What is the name of the new zone?

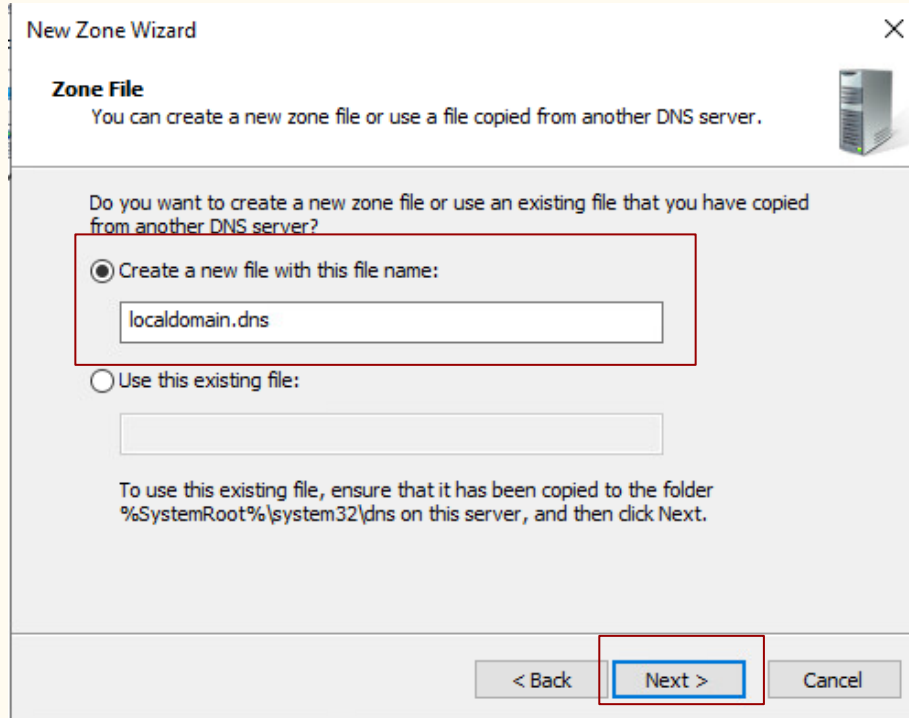
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:  
localdomain

< Back   Next >   Cancel

# DNS configurations.

The wizard will create the entries necessities for the database and a new file with the correct name. Just leave the default and select 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:

localdomain.dns

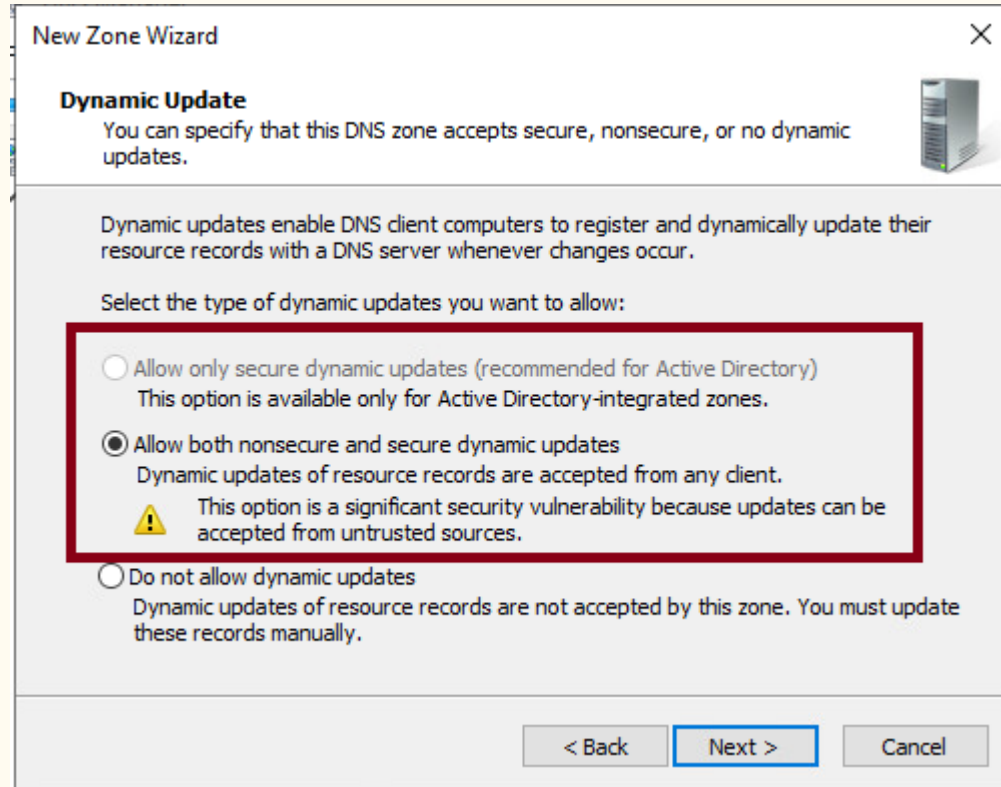
☐ Use this existing file:

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

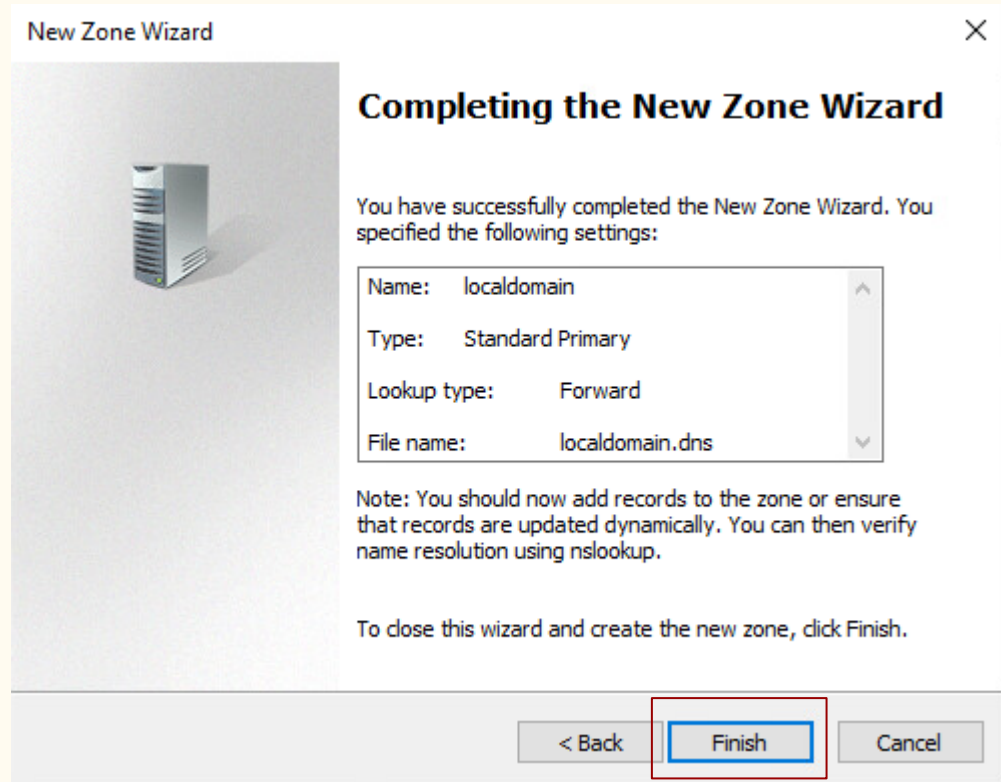
# DNS configurations.

The secure configuration will include allow only secure dynamic updates. This will be used by active directory. Since we don't install yet our AD, select the less secure allow both nonsecure and secure...



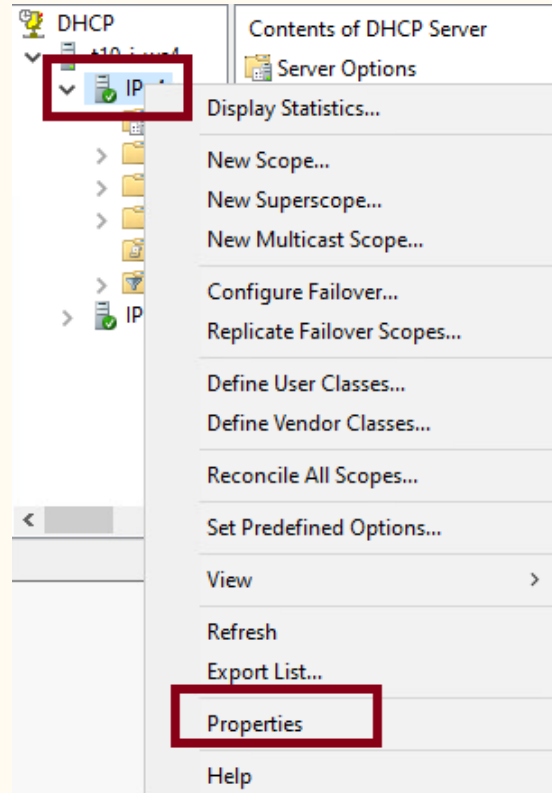
# DNS configurations.

This next window will present all the selected configurations and allow to finish the configuration.



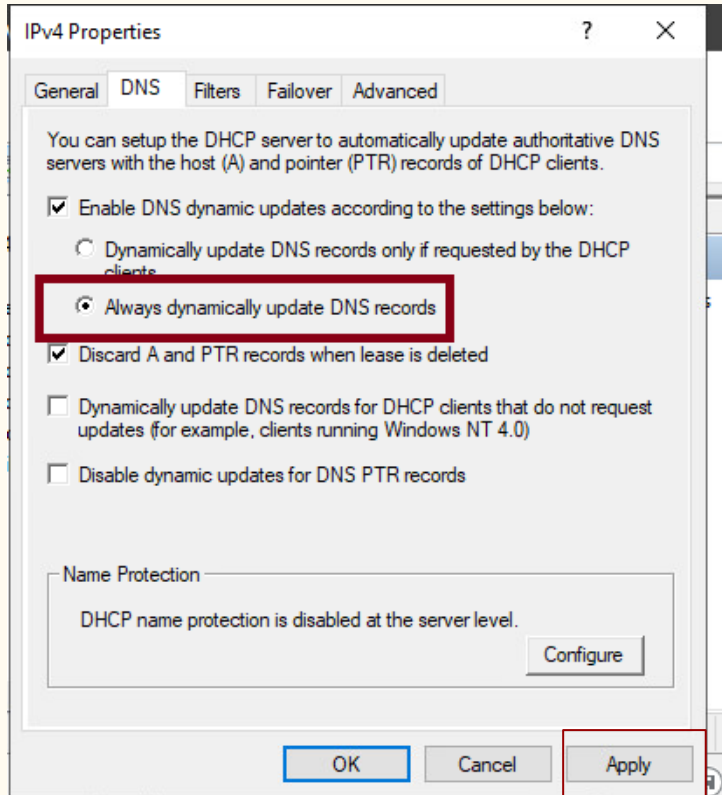
# DNS configurations to allow dynamic updates from DHCP.

Open DHCP manager  
and select the server,  
and go to properties.



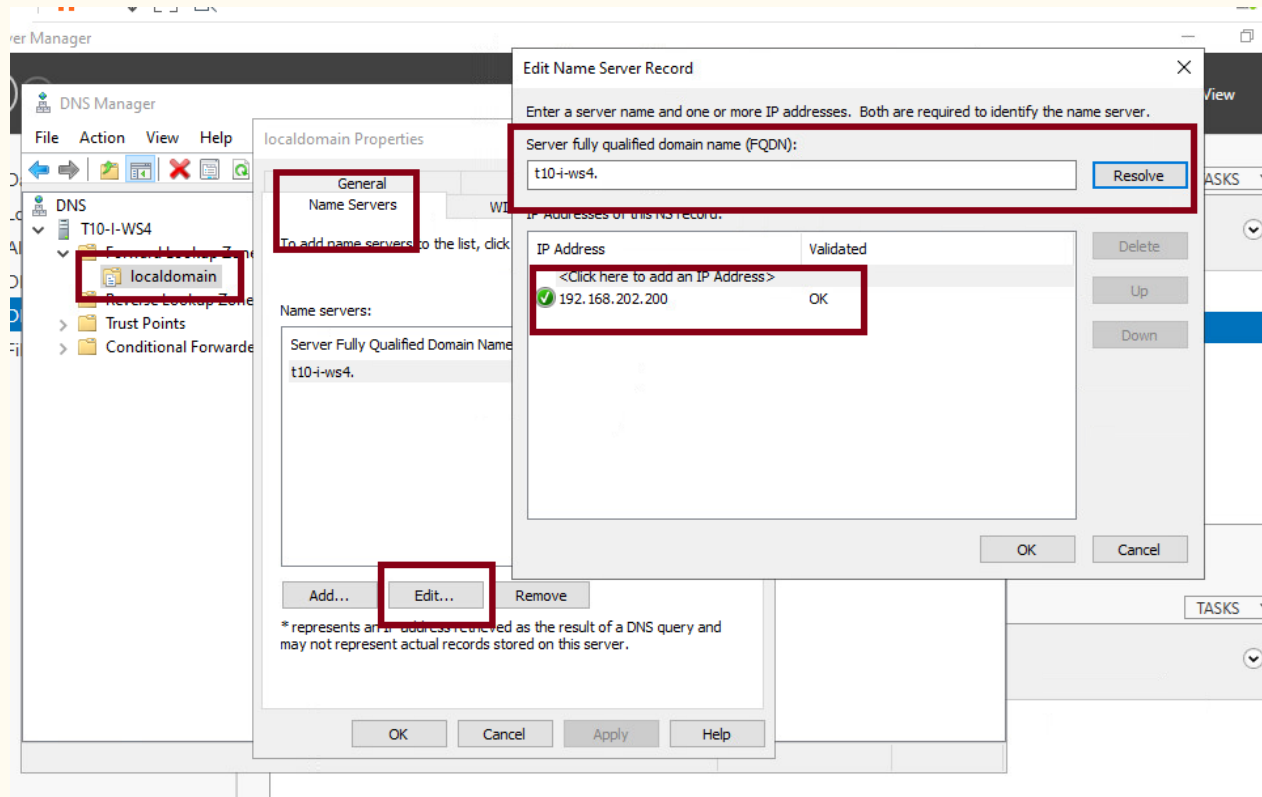
# DNS configurations to allow dynamic updates from DHCP.

On the DNS tab  
check that Always  
dynamically update  
DNS records is  
selected. Click Apply.



# DNS configurations to allow dynamic updates from DHCP.

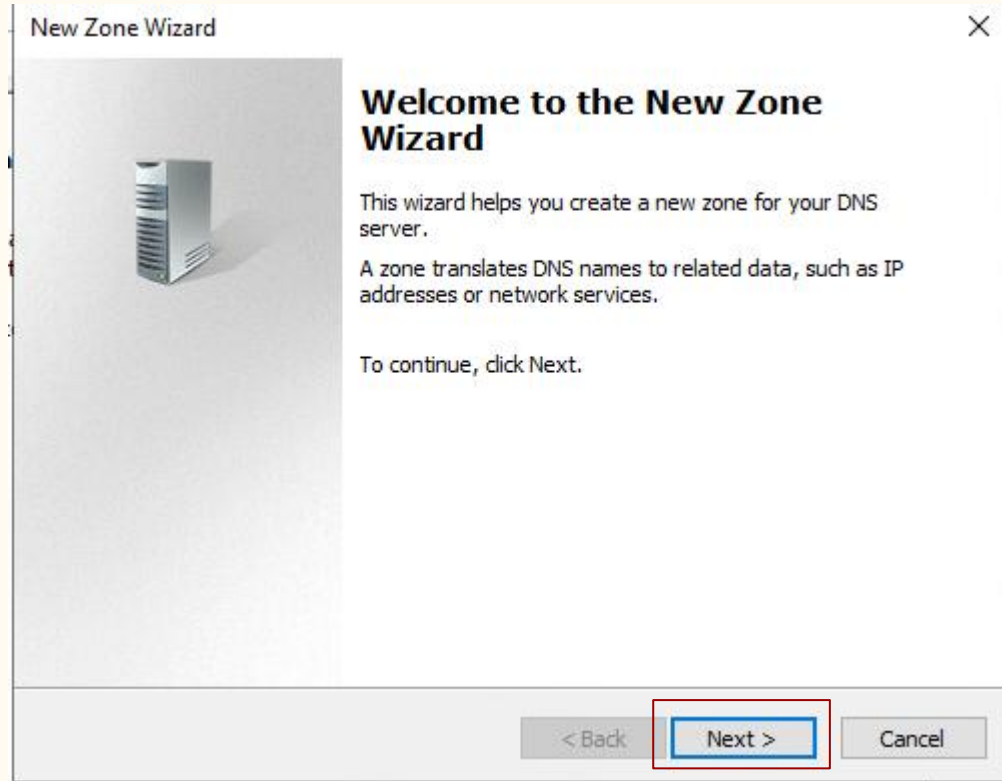
On DNS manager we select the domain and his properties and in general tab edit the server record. We set the name of the server, and the DNS will resolve his IP address. Click resolve to see how the DNS resolve his own address.





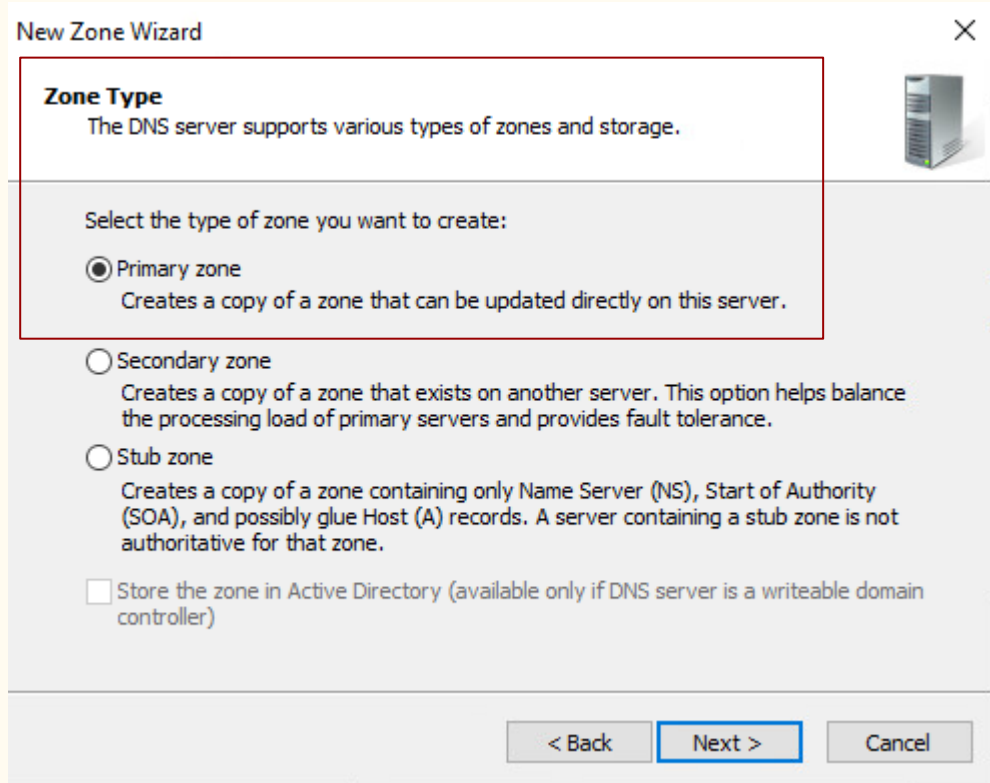
# Reverse lookup zones.

On the DNS manager select Reverse lookup zones in the same way you selected lookup zones. This will create a reverse lookup zone that will resolve names of machines into his ip's.



# Reverse lookup zones.

Select Primary zone.



New Zone Wizard

**Zone Type**  
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

☒ Primary zone  
Creates a copy of a zone that can be updated directly on this server.

☐ Secondary zone  
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

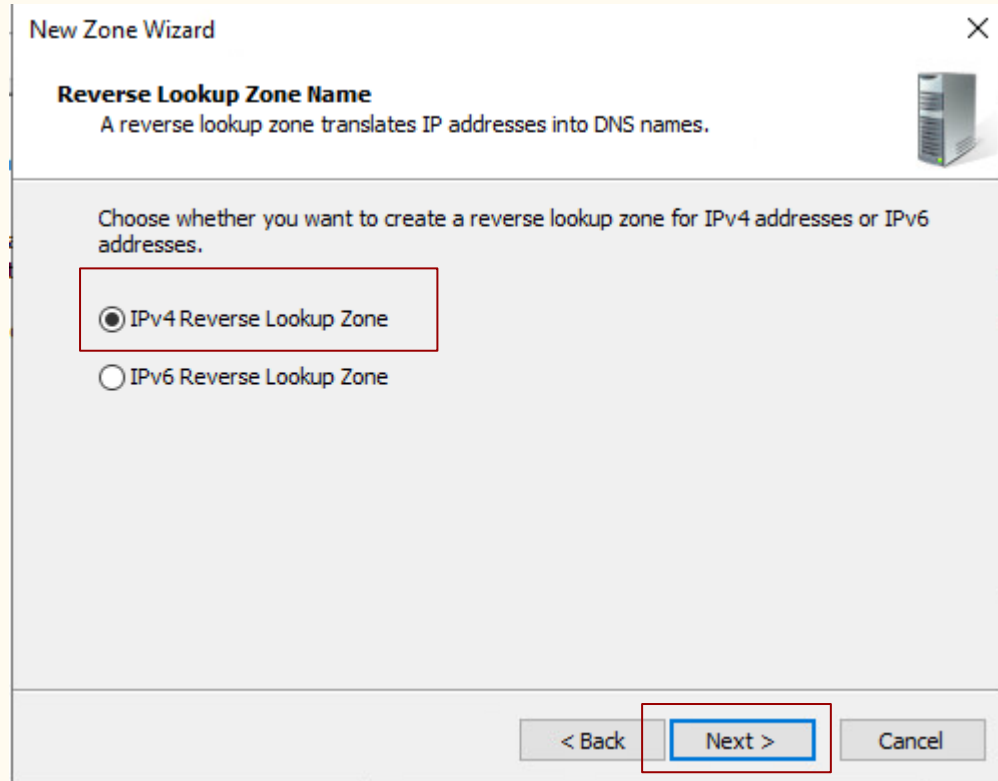
☐ Stub zone  
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☐ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back   Next >   Cancel

# Reverse lookup zones.

Select IPv4 Reverse Lookup Zone. Click next.

A screenshot of the 'New Zone Wizard' dialog box in Windows. The title bar says 'New Zone Wizard' with a close button. The main heading is 'Reverse Lookup Zone Name' with a subtext 'A reverse lookup zone translates IP addresses into DNS names.' and a server icon. Below this, it says 'Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.' There are two radio button options: 'IPv4 Reverse Lookup Zone' (which is selected and highlighted with a red rectangle) and 'IPv6 Reverse Lookup Zone'. At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (highlighted with a blue rectangle), and 'Cancel' (disabled).

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.

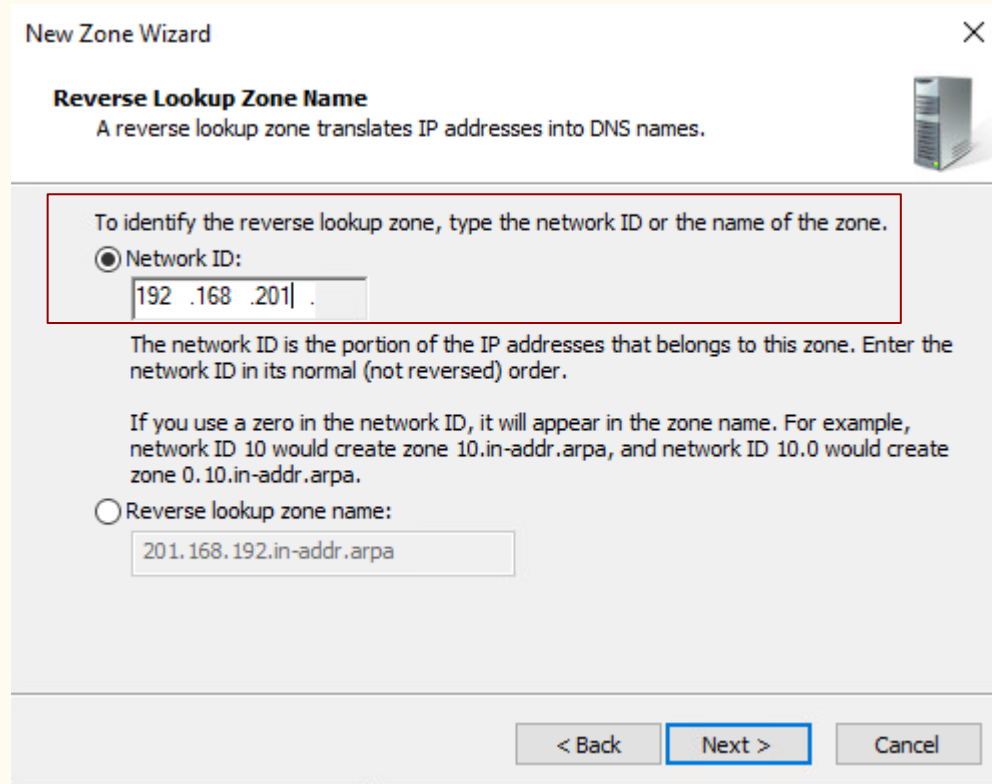
☒ IPv4 Reverse Lookup Zone

☐ IPv6 Reverse Lookup Zone

< Back   Next >   Cancel

# Reverse lookup zones.

Put the first 3 octet from the scope that you want to refer by this zone in network ID. Then 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:

192 .168 .201| .

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.

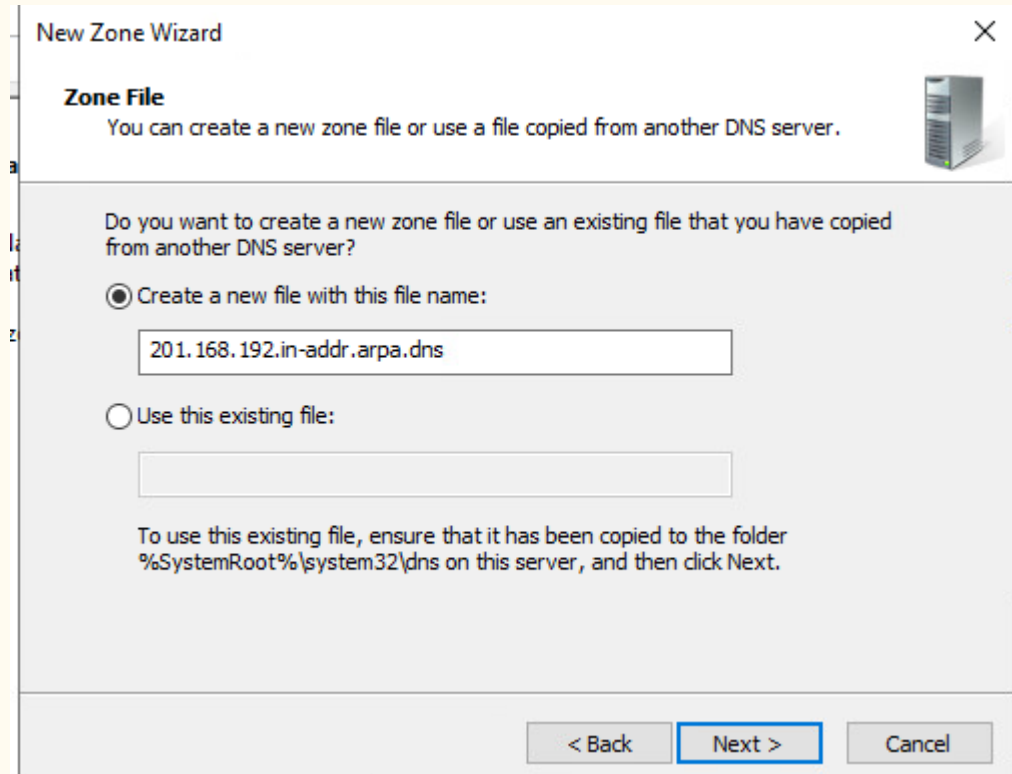
☐ Reverse lookup zone name:

201.168.192.in-addr.arpa

< Back   **Next >**   Cancel

# Reverse lookup zones.

The wizard will create the files necessary for this task. Leave the default settings and click next.



The screenshot shows the 'New Zone Wizard' dialog box, specifically the 'Zone File' step. The title bar reads 'New Zone Wizard' with a close button. Below the title, the section is labeled 'Zone File' with a sub-instruction: 'You can create a new zone file or use a file copied from another DNS server.' To the right of this text is a small icon of a server rack. The main area contains the question: 'Do you want to create a new zone file or use an existing file that you have copied from another DNS server?'. There are two radio button options: 'Create a new file with this file name:' (which is selected) and 'Use this existing file:'. The first option has a text input field containing '201.168.192.in-addr.arpa.dns'. The second option has an empty text input field. At the bottom, there is a note: 'To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.' The bottom of the dialog features three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

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:

201.168.192.in-addr.arpa.dns

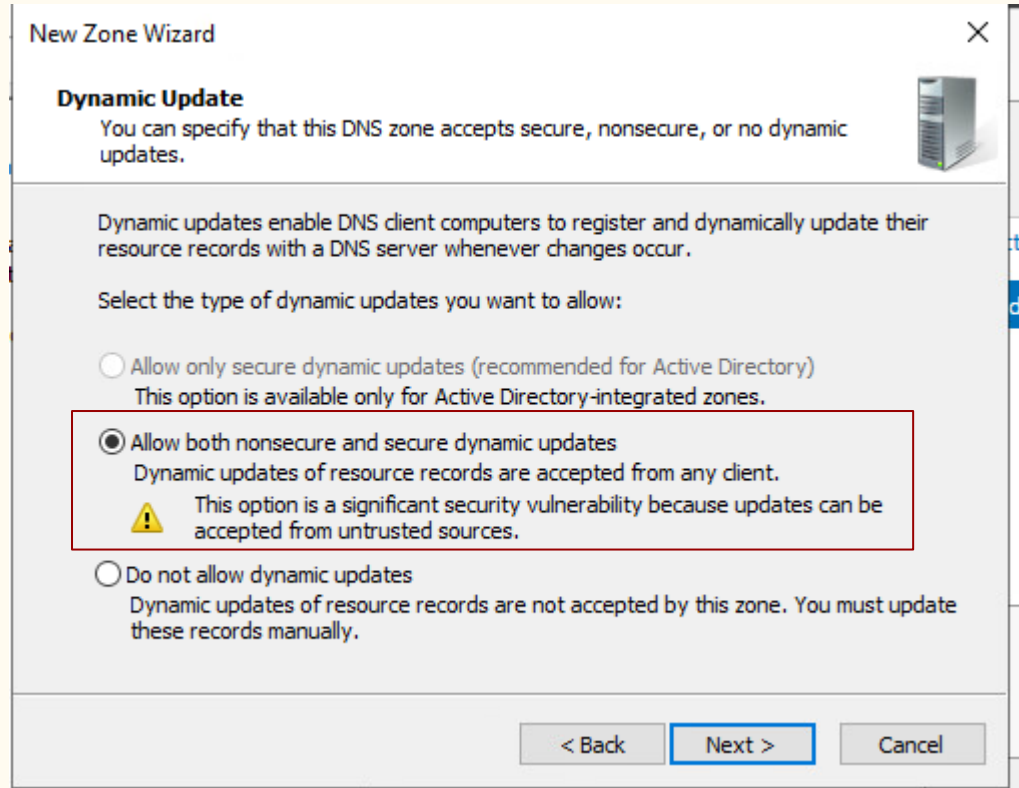
☐ Use this existing file:

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

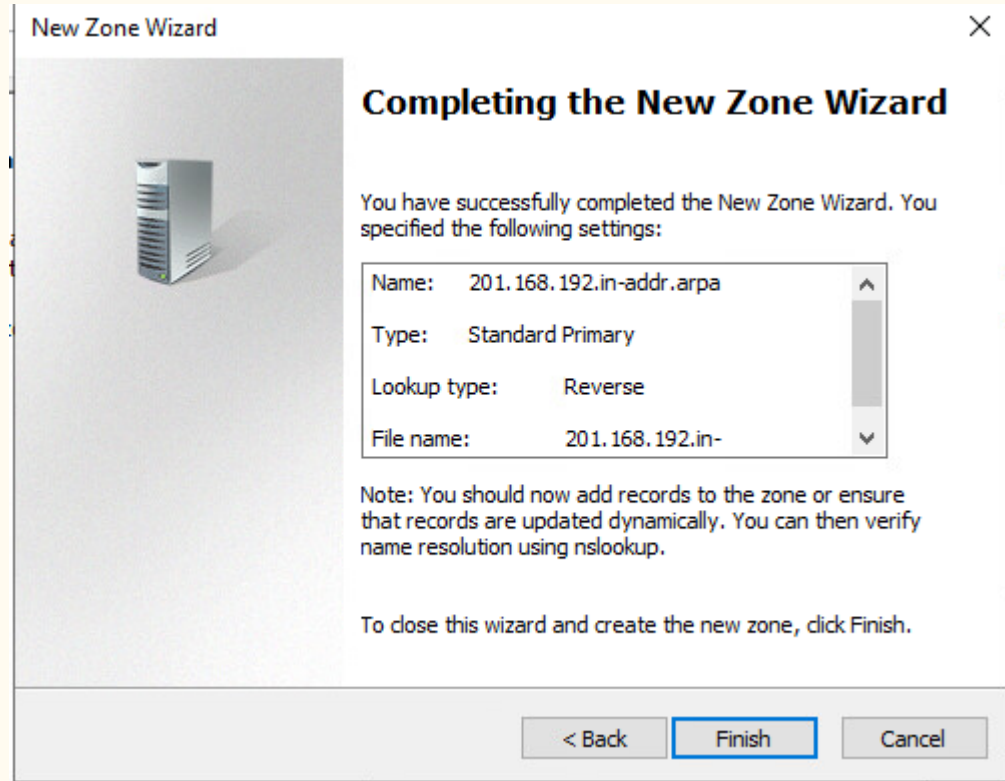
# Reverse lookup zones.

Again as we did with the forward zone select the less secure allow both... option.



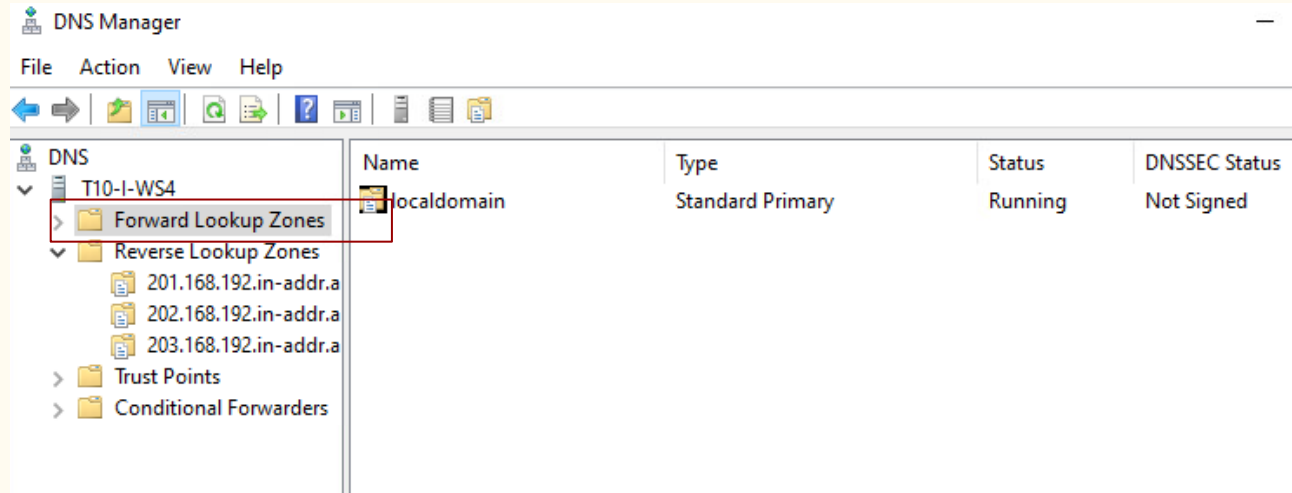
# Reverse lookup zones.

In the last window you will see the selected resumed configuration and you can select finish to create this zone.



# Check proper configurations.

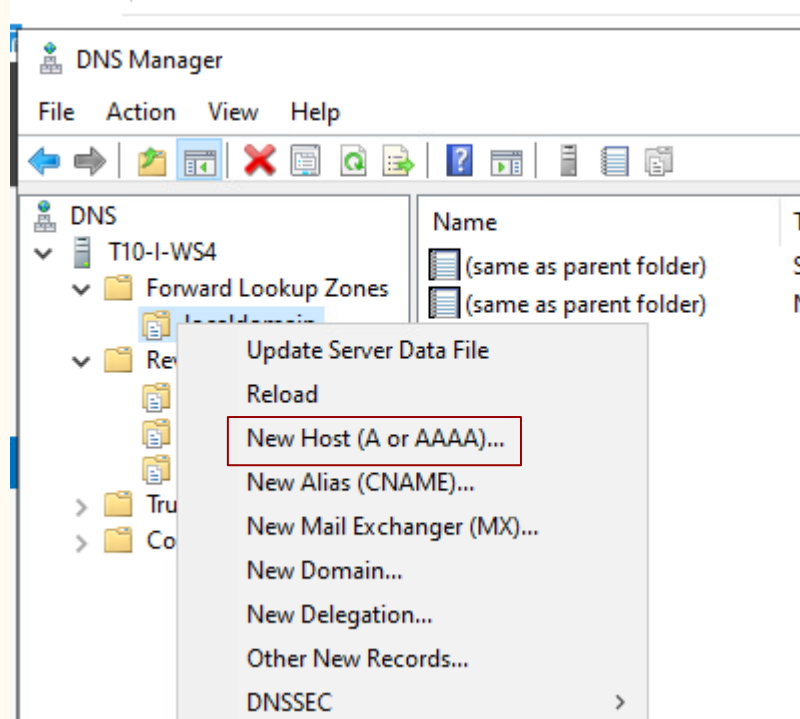
Since we have not leased any ip yet we can create a pointer to an address manually to check the resolution of the DNS server. On one of the scopes in DNS lookup zones right click and select new pointer(PTR). Set the host ip address and the host name. In this example we use a machine configured on the DMZ zone.





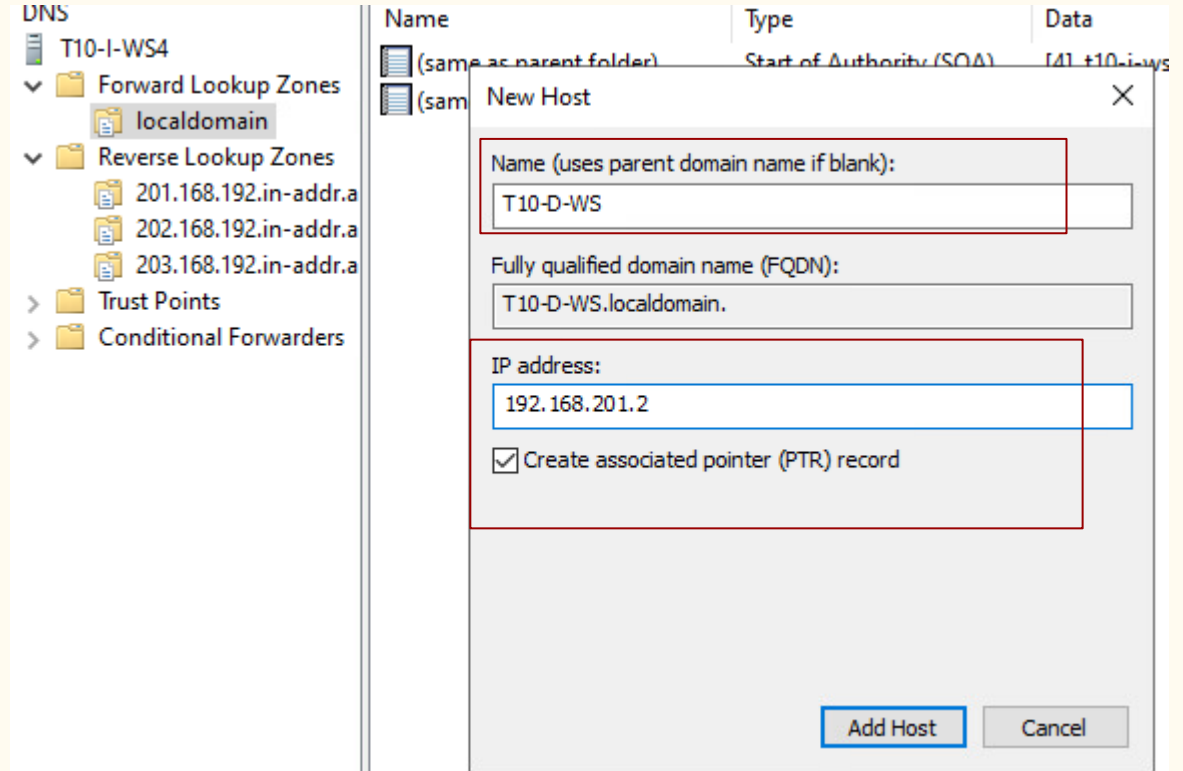
# Check proper configurations.

After right click in  
the forward zone  
select new host(A or  
AAAA)...



# Check proper configurations.

Fill up the required information. The name of the machine, and the ip address and select Create associated pointer. Finally click on add host.



The image shows a screenshot of the Windows DNS Manager console and a 'New Host' dialog box. In the DNS console, the tree view is expanded to 'Forward Lookup Zones' > 'localdomain'. The 'New Host' dialog box is open, showing the following fields and options:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[41] +10-i-ys
(sam		

**New Host** [X]

Name (uses parent domain name if blank):  
T10-D-WS

Fully qualified domain name (FQDN):  
T10-D-WS.localdomain.

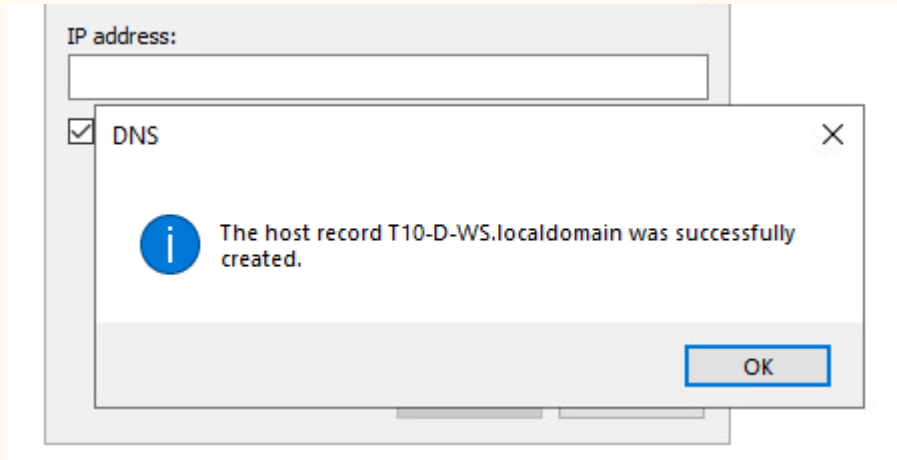
IP address:  
192.168.201.2

☒ Create associated pointer (PTR) record

Add Host Cancel

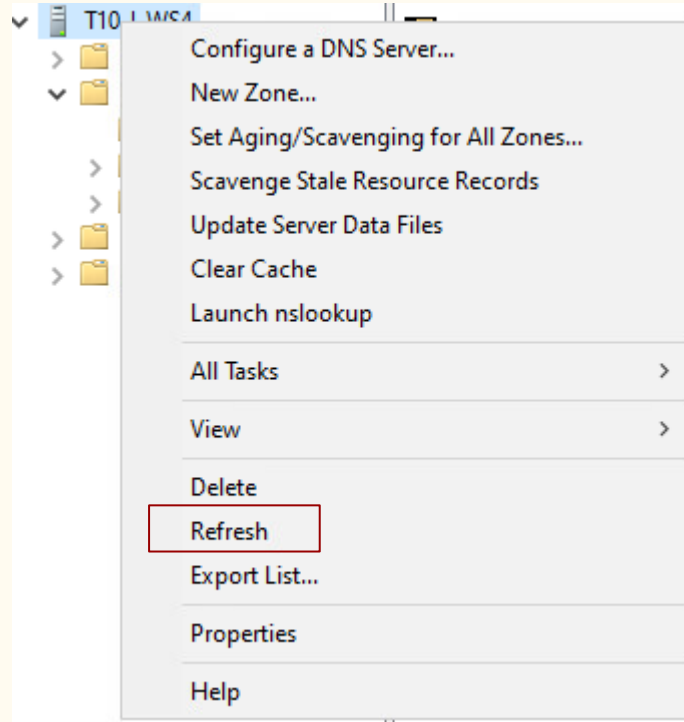
# Check proper configurations.

This message of successful updating will appear. However if you check your reverse zone the pointer has not yet being created.



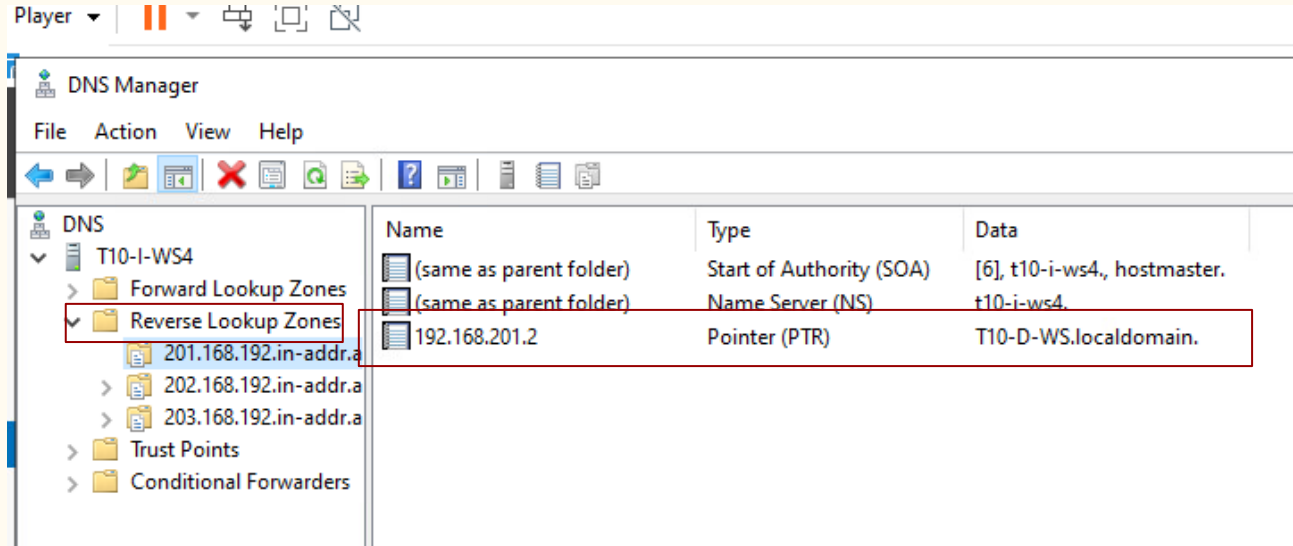
# Check proper configurations.

Go to the server icon  
right click and select  
refresh to update the  
database with the  
new pointer. That  
will update the  
reverse lookup zone.



# Check proper configurations.

Here you can see the newly created reverse pointer. We can now check this configuration changes by using nslookup in a powershell.



# Check proper configurations.

Here we can see the result of looking with nslookup on the database of DNS in this machine. It resolves both the ip address and the name of the machine into an ip.

```
PS C:\Users\cgarcia> nslookup
Default Server:  localhost
Address:  127.0.0.1

> 192.168.201.2
Server:  localhost
Address:  127.0.0.1

Name:    T10-D-WS.localdomain
Address:  192.168.201.2

> T10-D-WS.localdomain
Server:  localhost
Address:  127.0.0.1











Name:    T10-D-WS.localdomain
Address:  192.168.201.2

> -
```

Activate Windows  
Go to Settings to activate  
Windows.

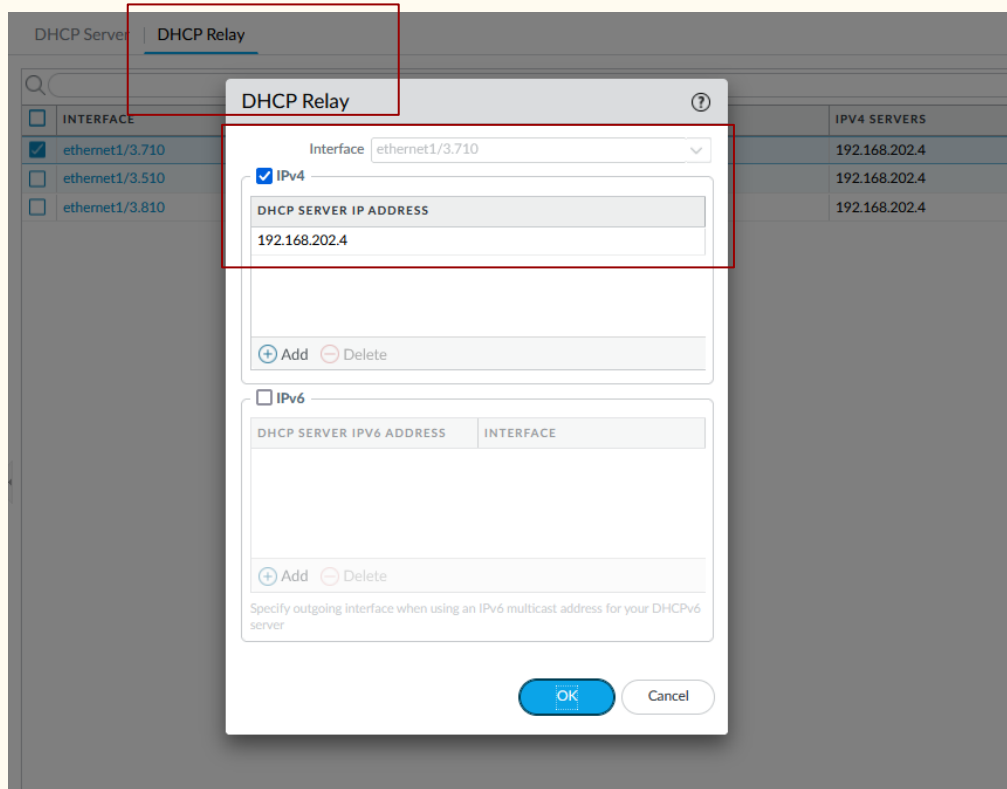
# Configurations to allow DHCP broadcast through firewalls.

First approach was to allow those broadcast through the firewall policies on secure tab, without results.

				interconnect								
12	allow-hdcp-traffic-responses	none	universal	 inside	 192.168.202.4	any	any	 dmz	any	any	 dhcp	 af
								 interconnect				
13	allow-dhcp-traffic-requests	none	universal	 dmz	any	any	any	 inside	any	any	any	 af
				 interconnect								

# Configurations to allow DHCP broadcast through firewalls.

After an internet search we found that has to create DHCP relays on the interfaces. This relays receive the broadcast and forwarder to the different zones from and to the DHCP. On the Network tab in the Palo Alto we select from the right menu DHCP, and then relay. We choose each different interface and create a new relay for each one pointing towards our DHCP server. In this example the address is 192.168.202.4. In our configuration should be 192.168.202.200.





# Configurations to allow DHCP broadcast through firewalls.

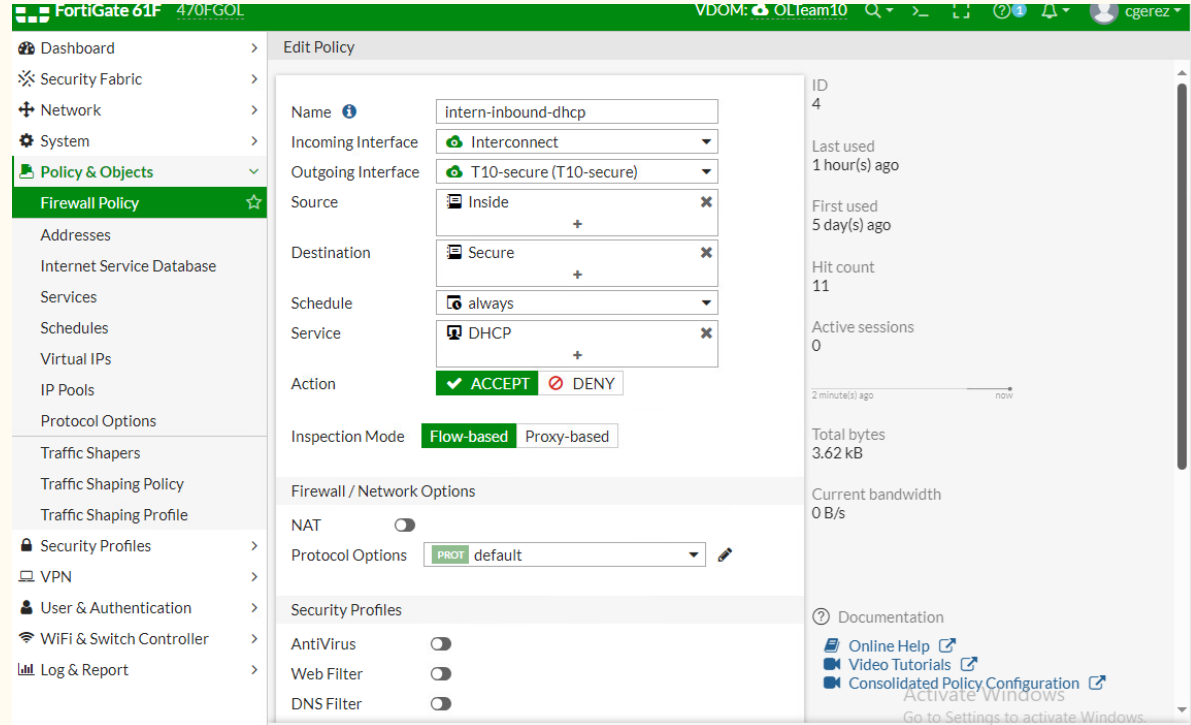
This is how looks like the network dhcp Relay tab after our configurations. Look at the path to the right tabs.

The screenshot displays the configuration interface for a PA-440 device. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The NETWORK tab is selected and highlighted with a red box. On the left sidebar, the DHCP option is highlighted with a red box. The main content area shows the DHCP Server configuration, with the DHCP Relay tab selected and highlighted with a red box. Below this, a table lists the configured DHCP relay interfaces.

INTERFACE	IPV4 ENABLED	IPV4 SERVERS	IPV6 ENABLED
<input type="checkbox"/> ethernet1/3.710	<input checked="" type="checkbox"/>	192.168.202.4	<input type="checkbox"/>
<input type="checkbox"/> ethernet1/3.510	<input checked="" type="checkbox"/>	192.168.202.4	<input type="checkbox"/>
<input type="checkbox"/> ethernet1/3.810	<input checked="" type="checkbox"/>	192.168.202.4	<input type="checkbox"/>

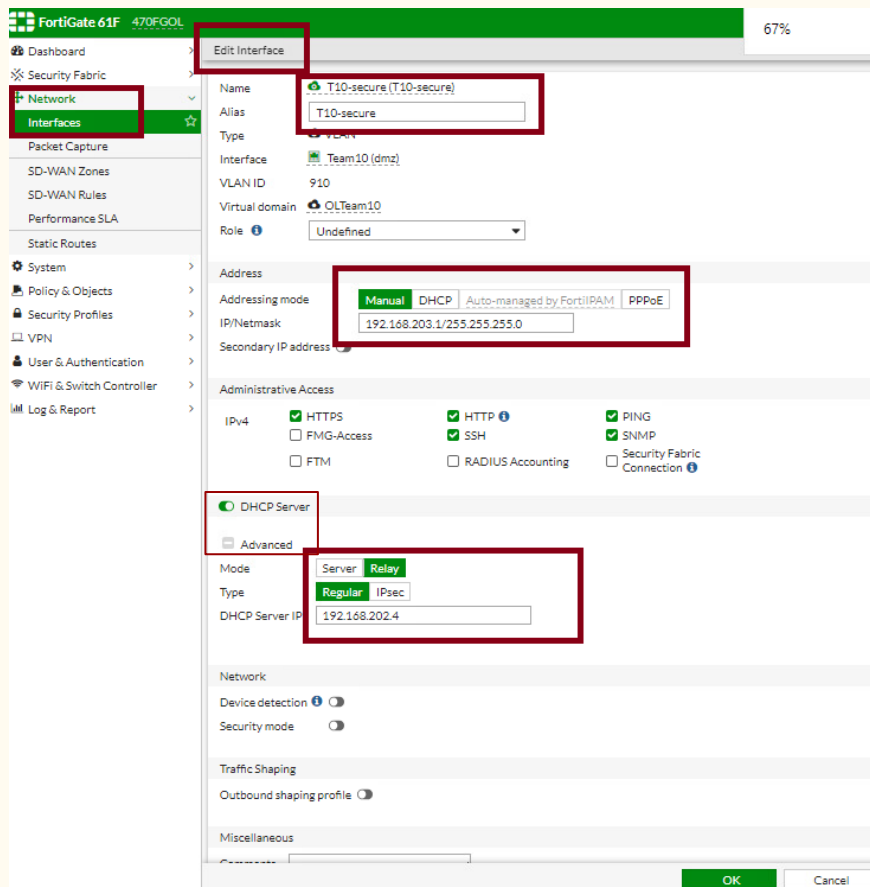
# Configurations to allow DHCP broadcast through firewalls.

In the same way we created firewall rules on the FortiGate firewall to allow broadcast to the secure zone. That of course didn't work well.



# Configurations to allow DHCP broadcast through firewalls.

We have the settings for DHCP relays by selecting each interface and allow the tab dhcp server, advance, and select relay. There we set the ip address of the DHCP server to allow broadcast to and from that address into the secure zone. We repeat the process for each interface.



# Configurations to allow DHCP broadcast through firewalls.

Looking at the interface final configuration we can see under DHCP ranges the relay configuration. That allow DHCP to reach all the zones inclusive the secure from the intern zone.

	Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Virtual Domain	Ref.
Physical Interface 3									
	Team10 (dmz)	Physical Interface		0.0.0.0/0.0.0.0			Relay: 192.168.202.4	OLTeam10	2
	Interconnect	VLAN		192.168.200.2/255.255.255.0	PING		Relay: 192.168.202.4	OLTeam10	7
	T10-secure (T10-secure)	VLAN		192.168.203.1/255.255.255.0	PING HTTPS SSH SNMP HTTP		Relay: 192.168.202.4	OLTeam10	5