DNS and DHCP in a Windows server.

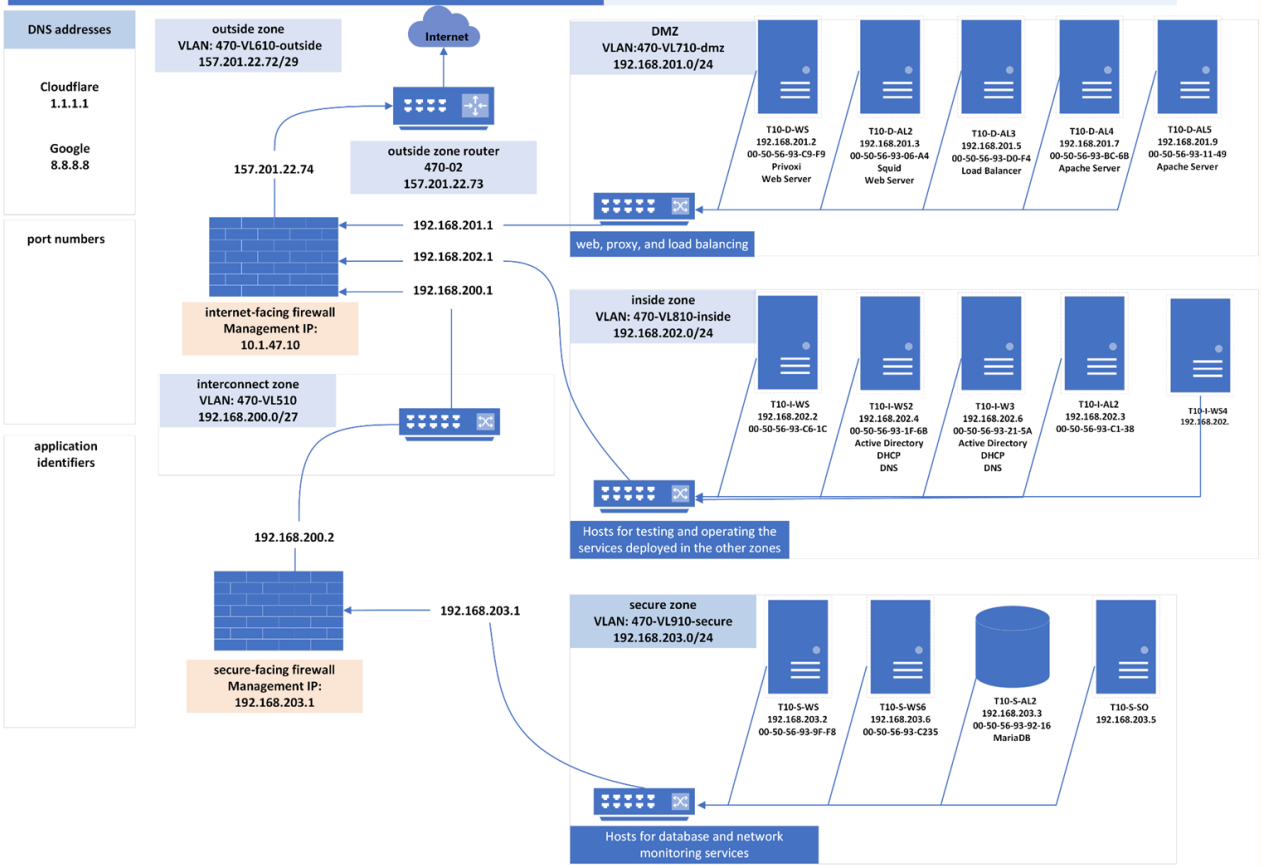
—

Carlos Gerez

cit470
Task: Diagram

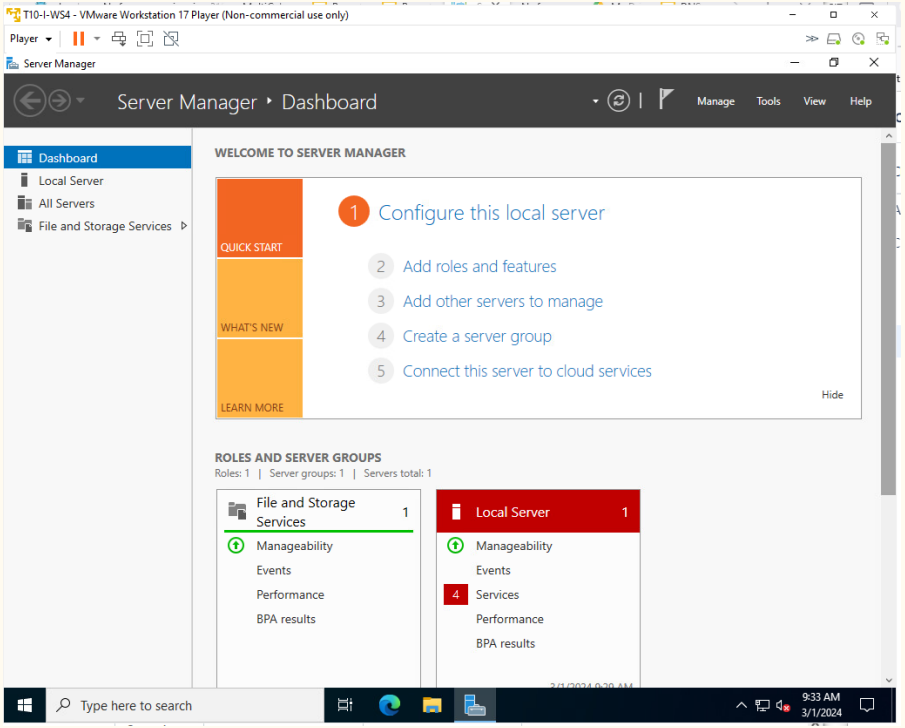
Team 10 Layer 3: outside zones' public IPv4 address assignments

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



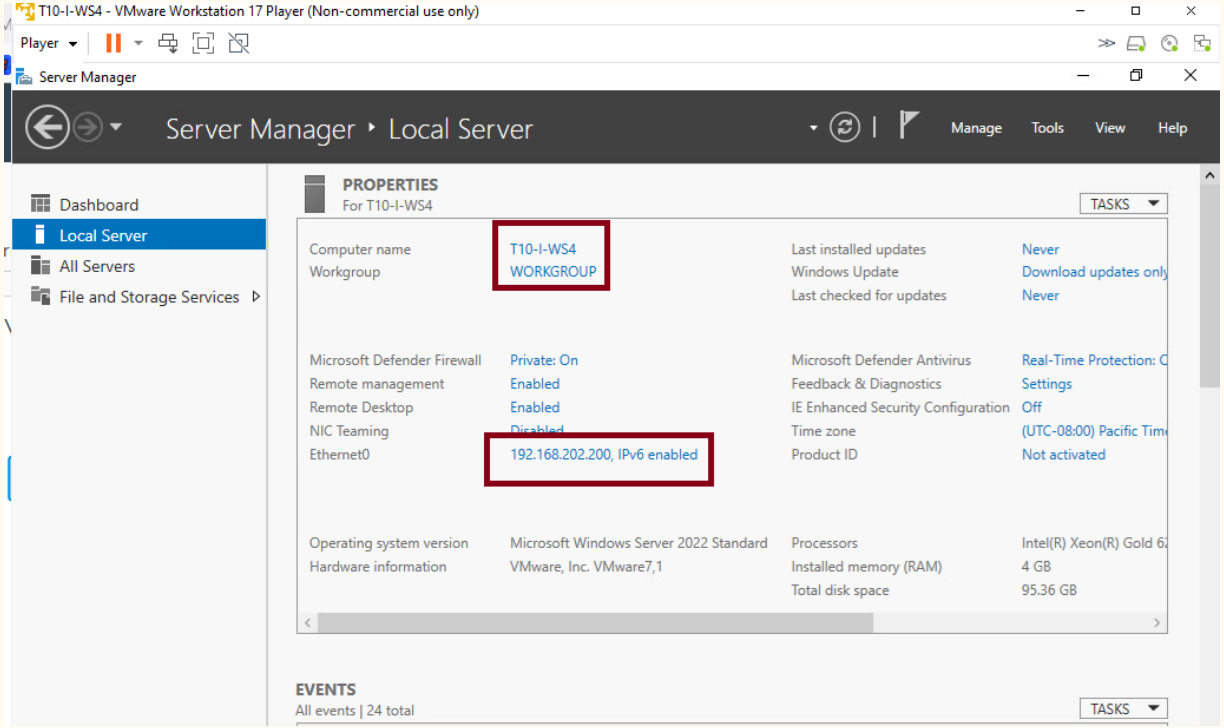
In order to configure the DHCP and DNS on our network I create a new testing server to install and configure DHCP and DNS.

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



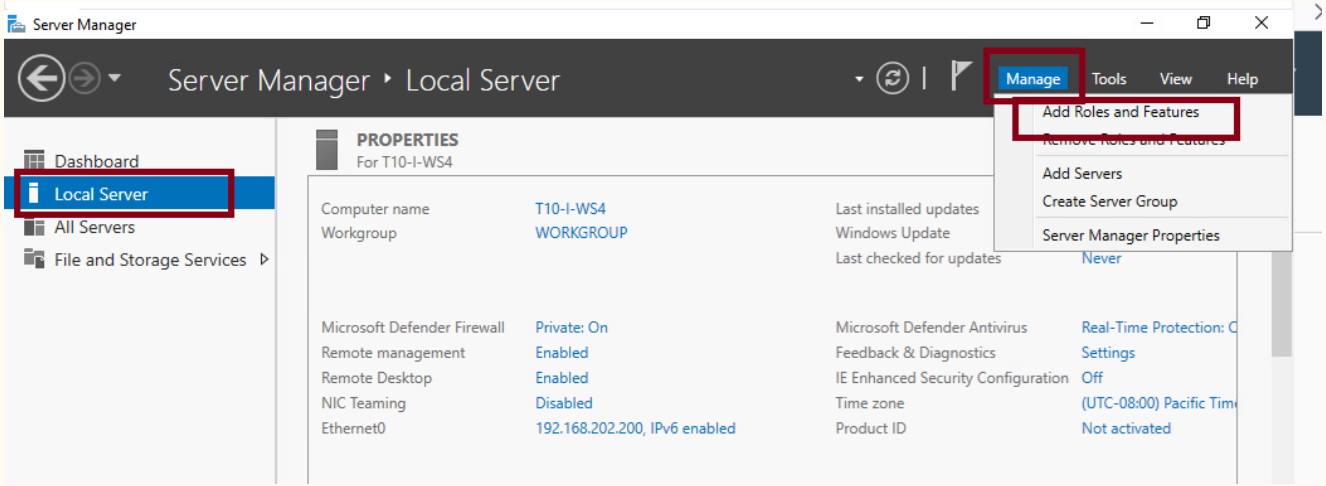
For this the Windows server is in the intern zone since it has to provide ips to the DMZ and the secure zone.

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



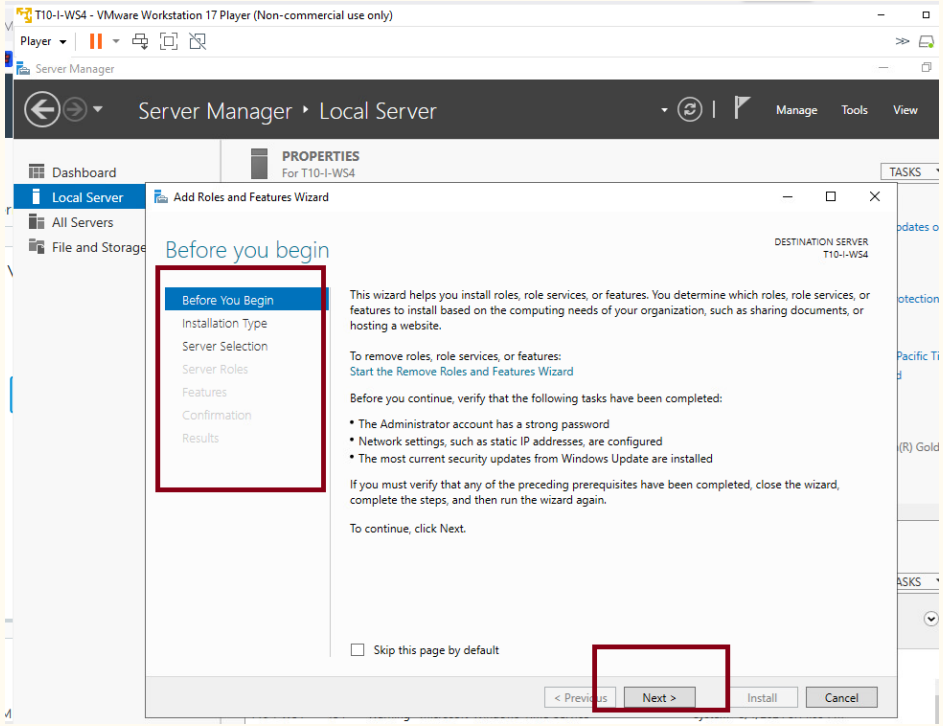
Configuration of features.

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



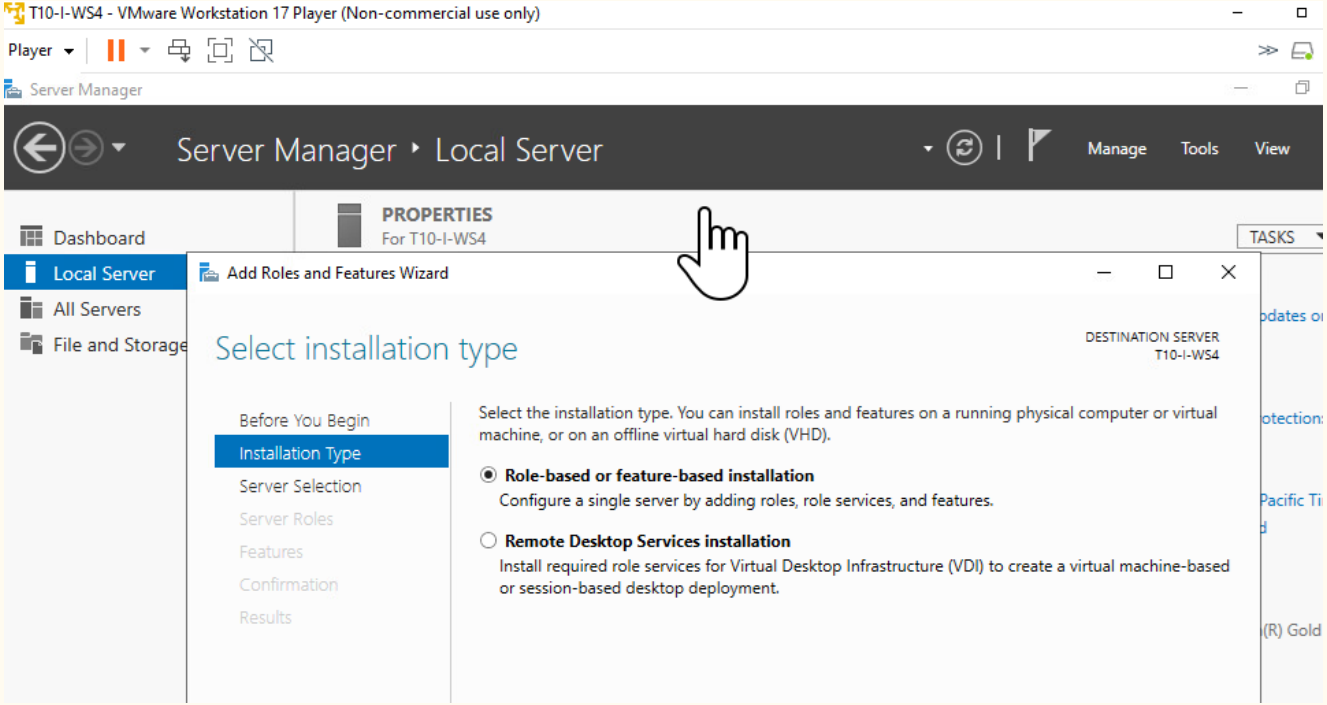
Configuration of features.

The interface will guide you through the process of installation.



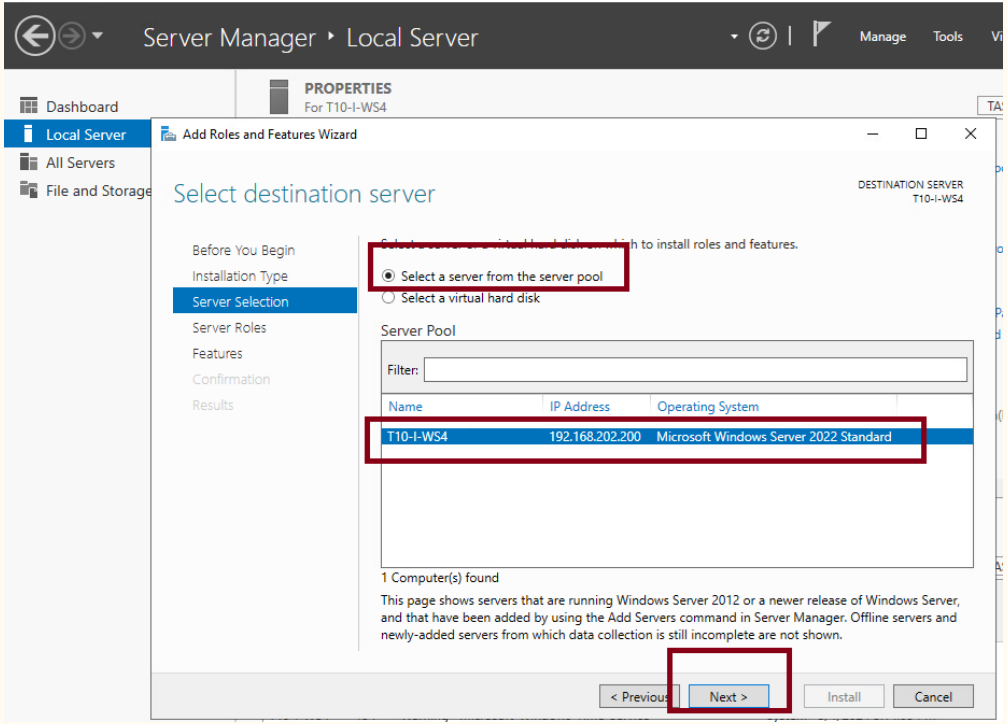
Configuration of features.

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



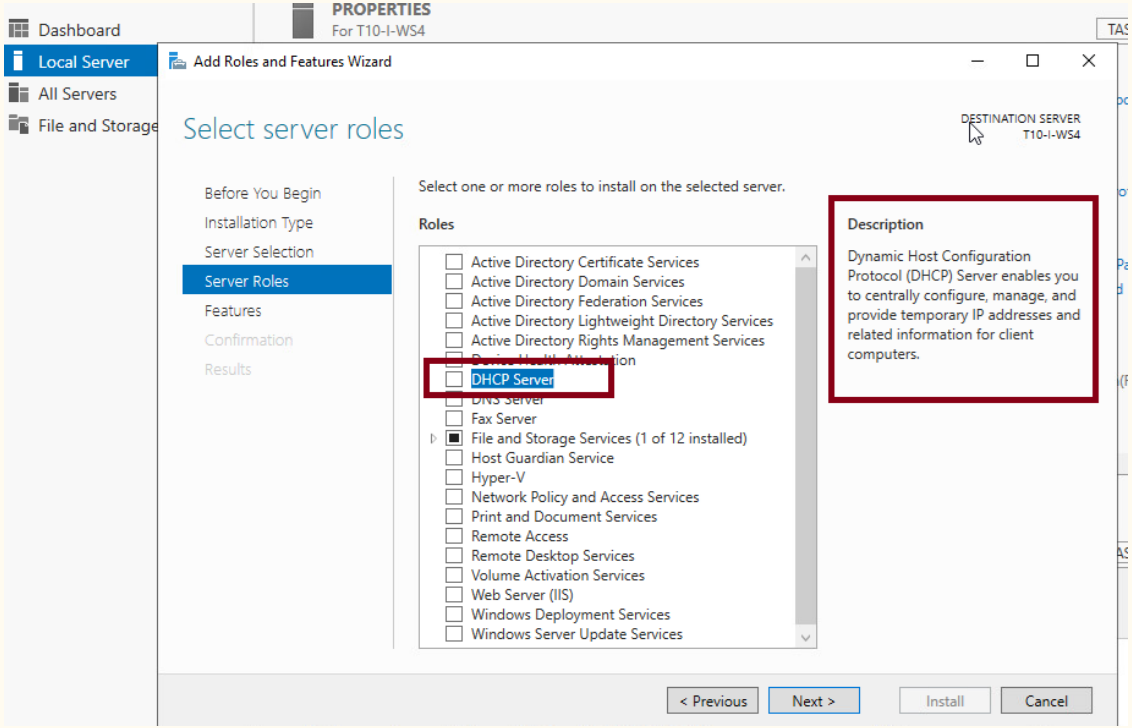
Configuration of features.

On server selection select your server.



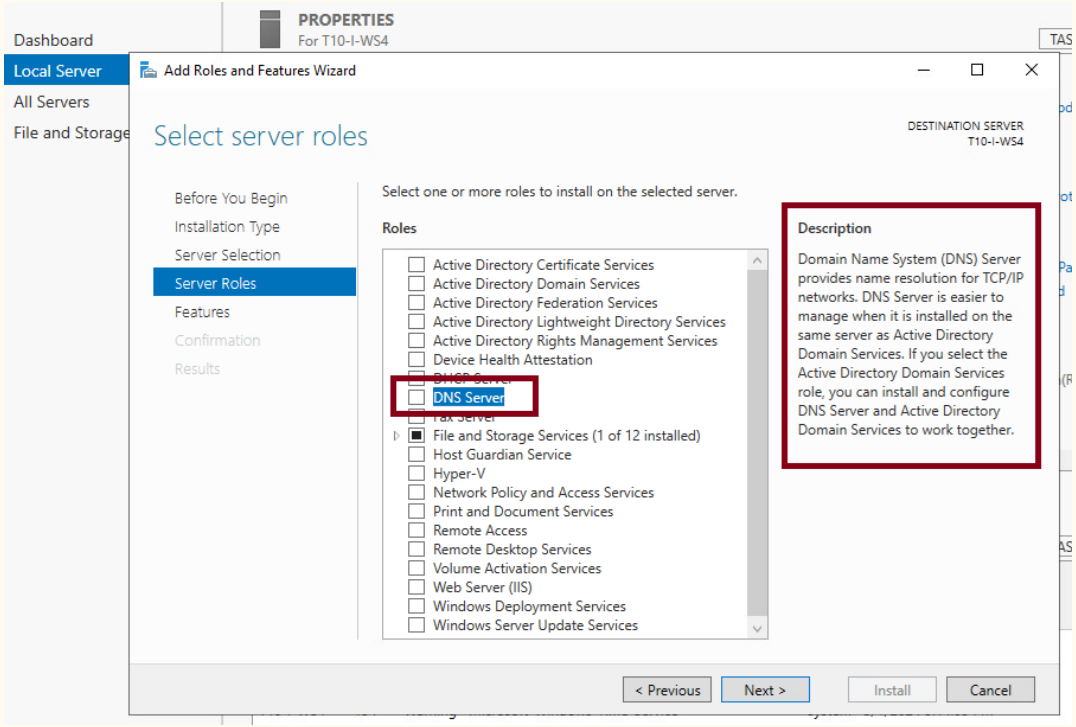
Configuration of features.

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



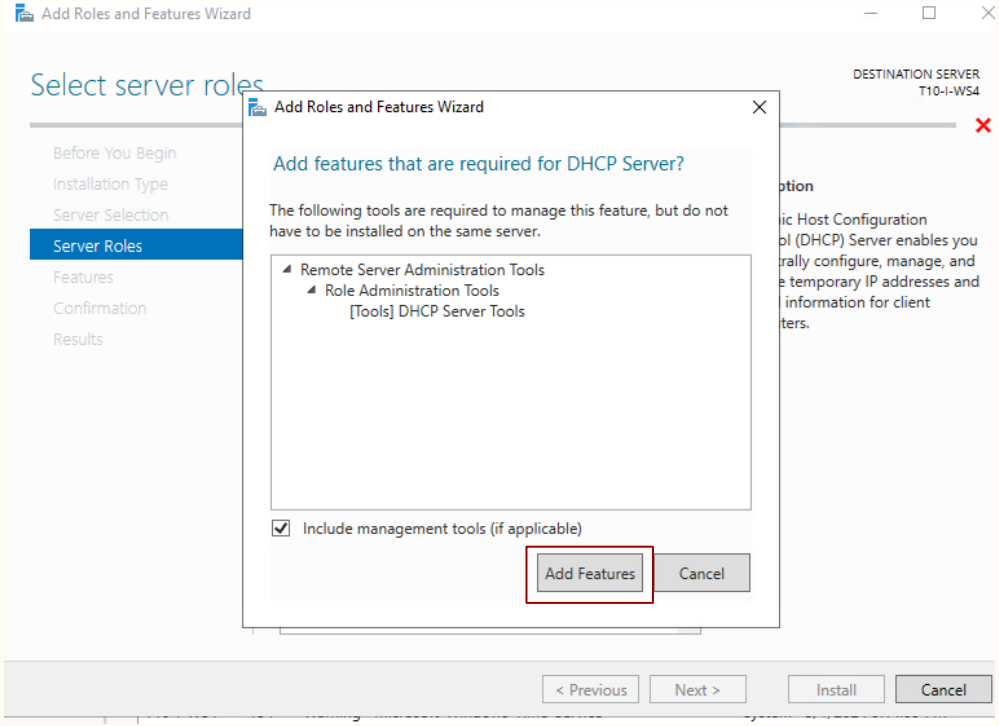
Configuration of features.

Select also here DNS Server, and read the description.



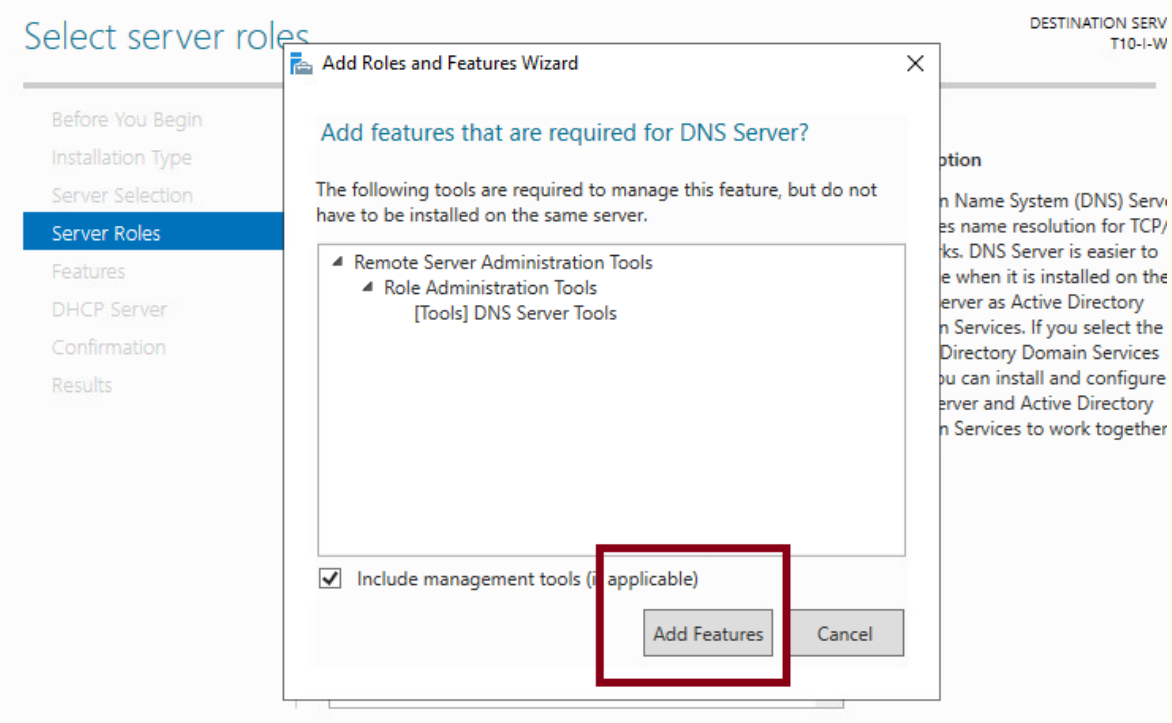
Configuration of features.

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



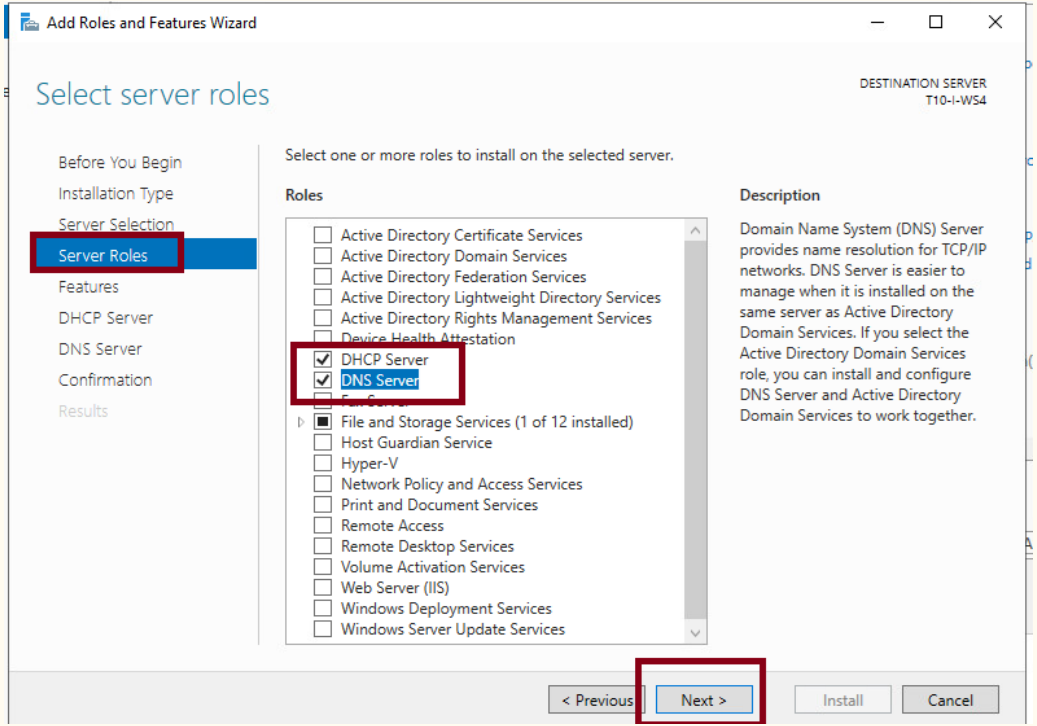
Configuration of features.

Do the same with DNS role.



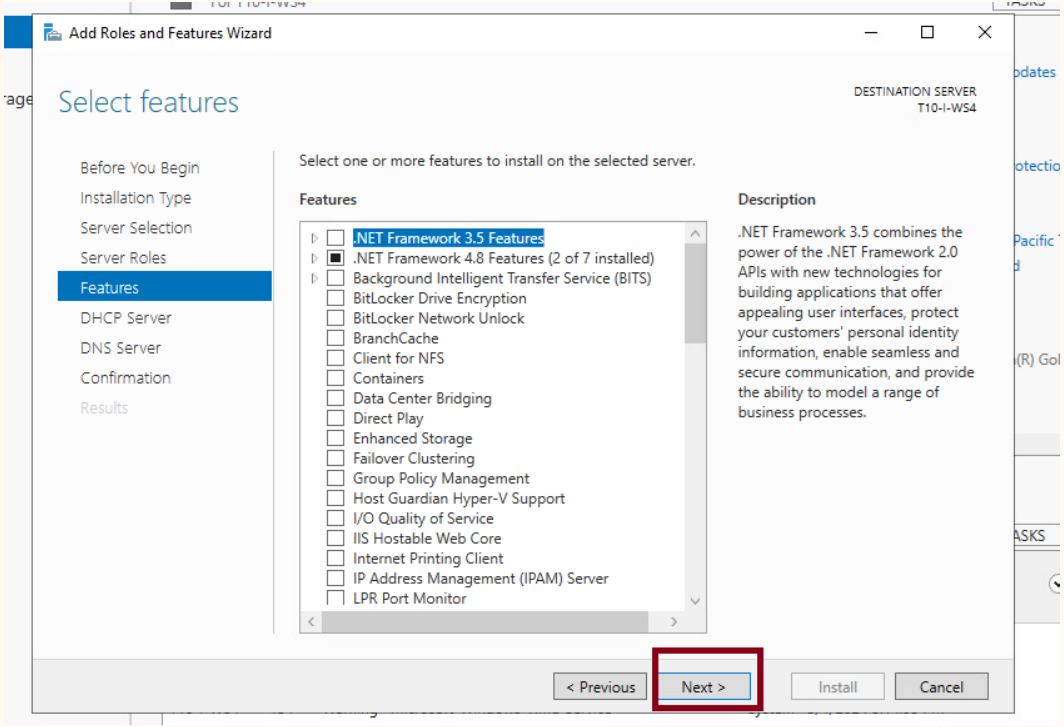
Configuration of features.

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



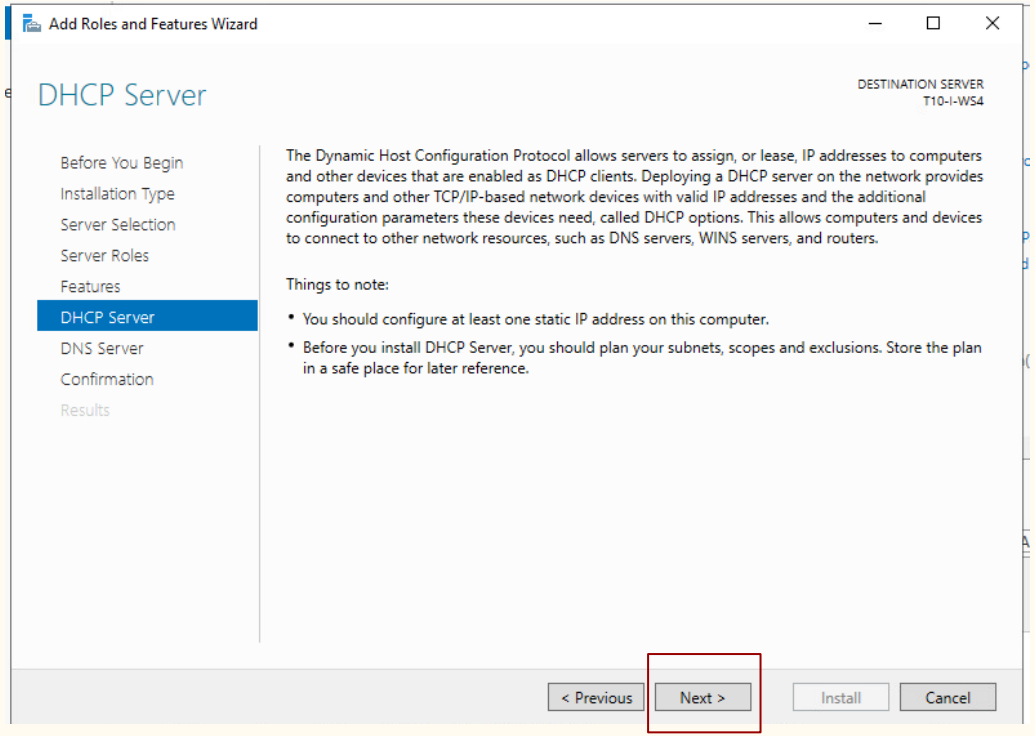
Configuration of features.

On features click next.



Configuration of features.

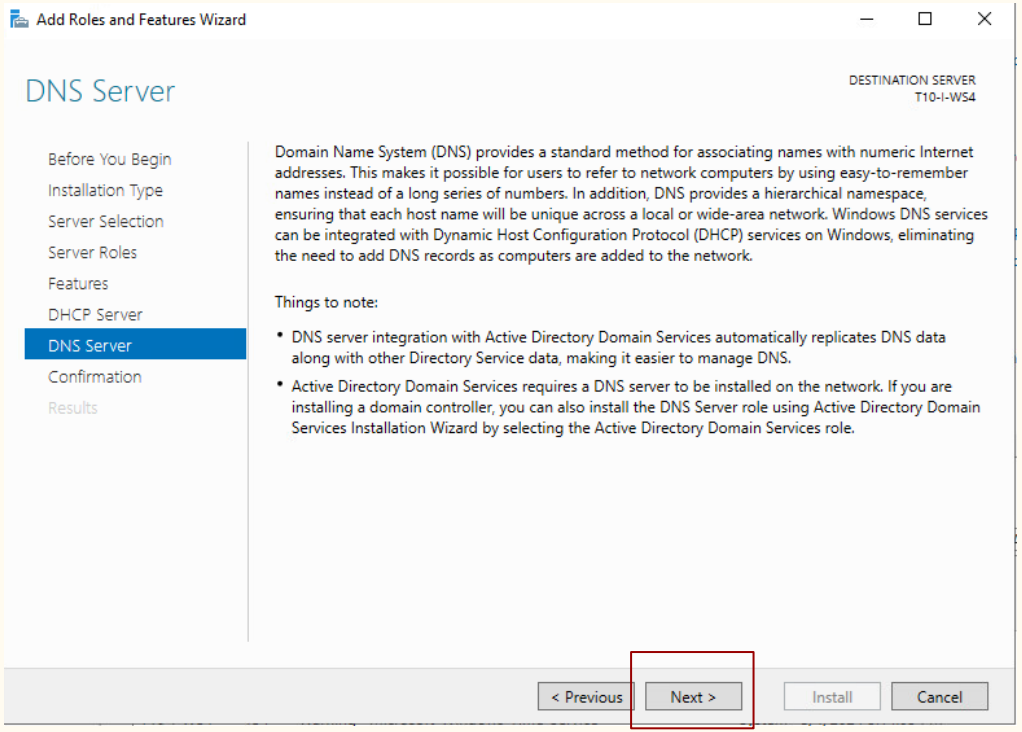
Select next after reading this description and notes.



Configuration of features.

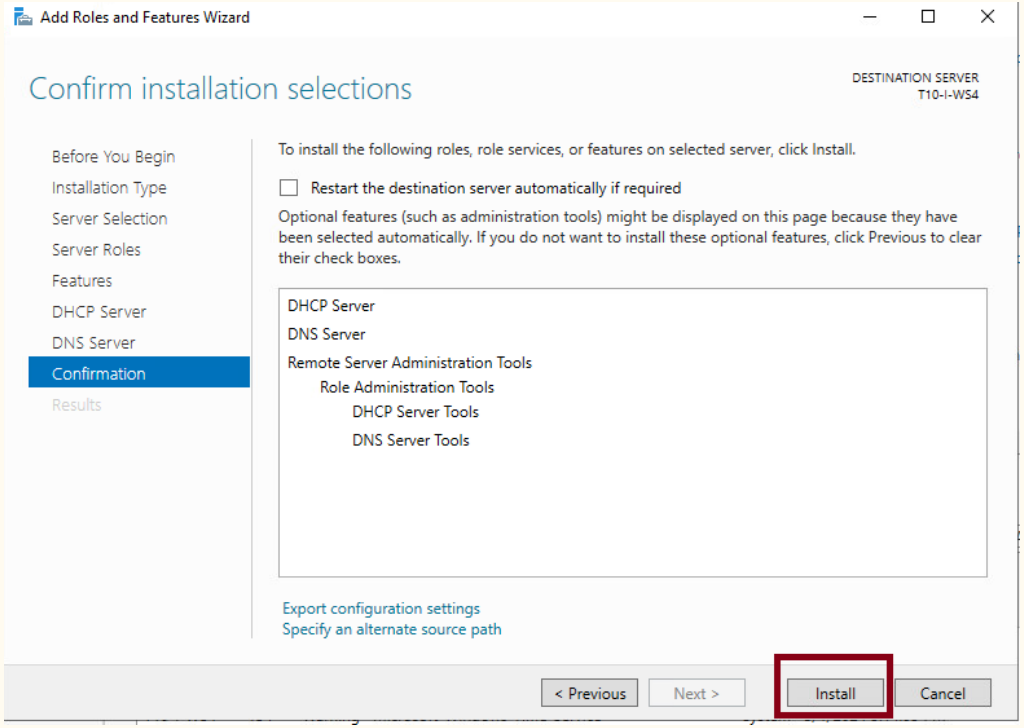
Select next after read the DNS information and things to note.

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.



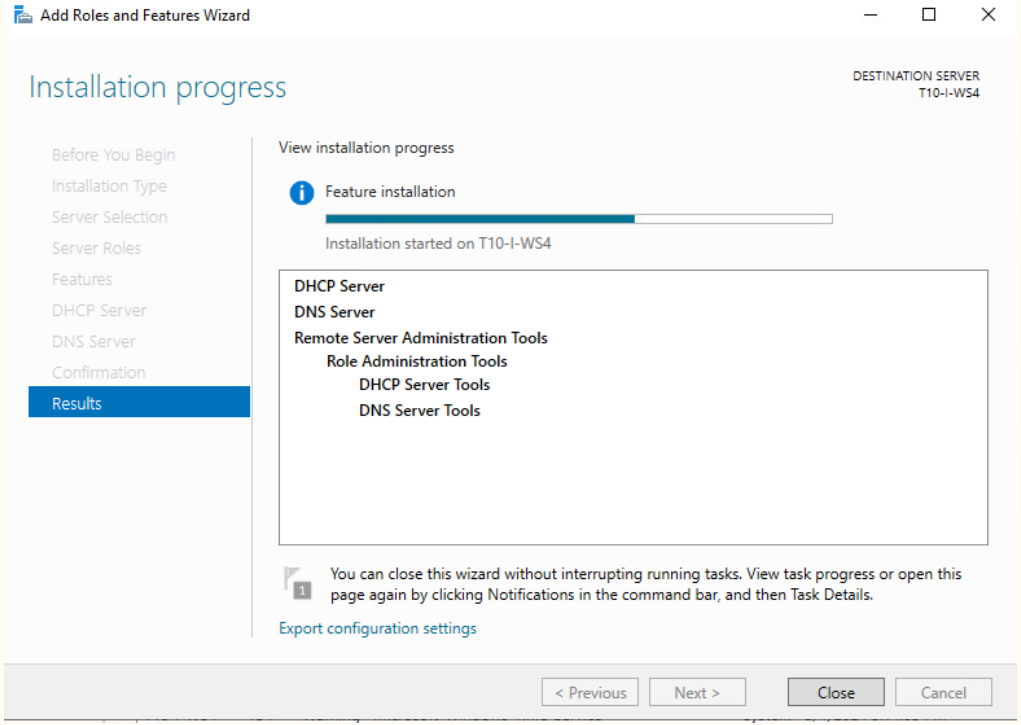
Configuration of features.

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



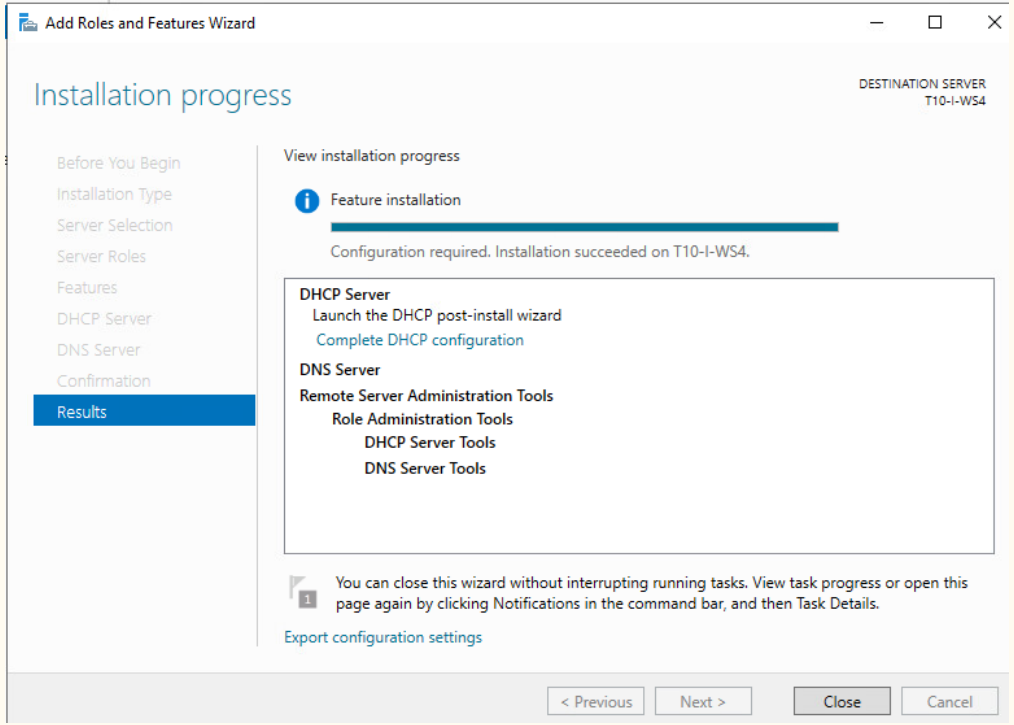
Configuration of features.

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



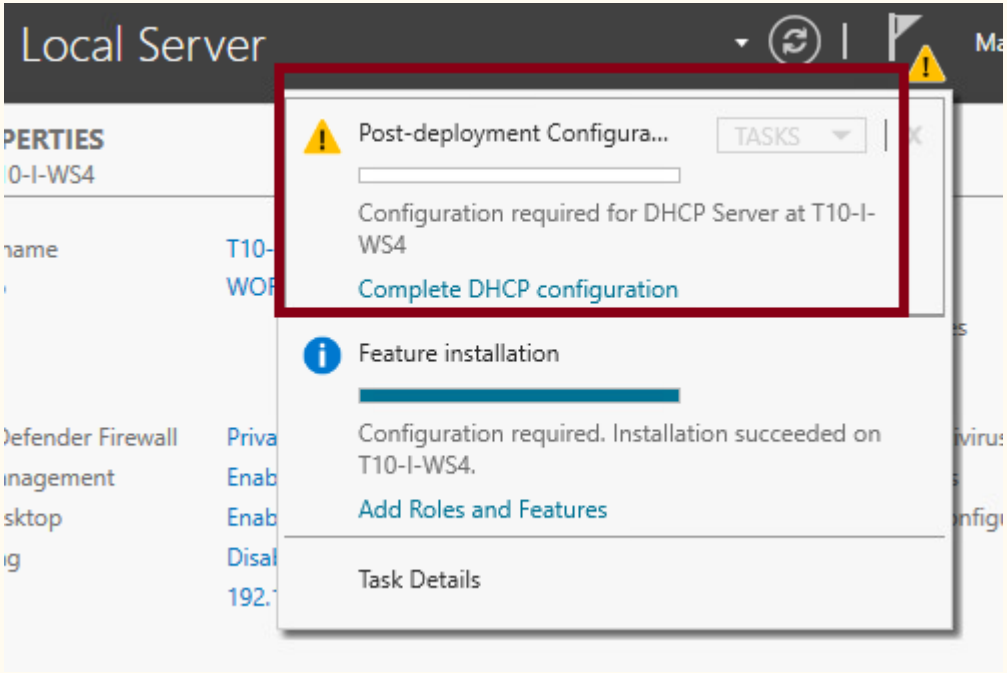
Configuration of features.

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



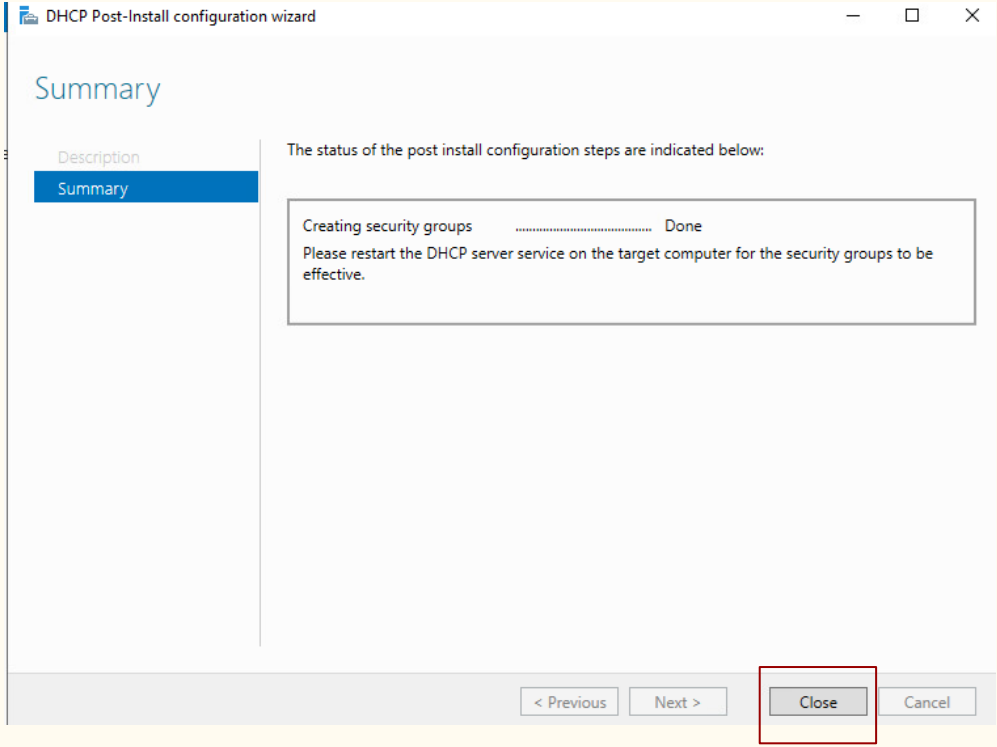
Post-deployment configurations

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



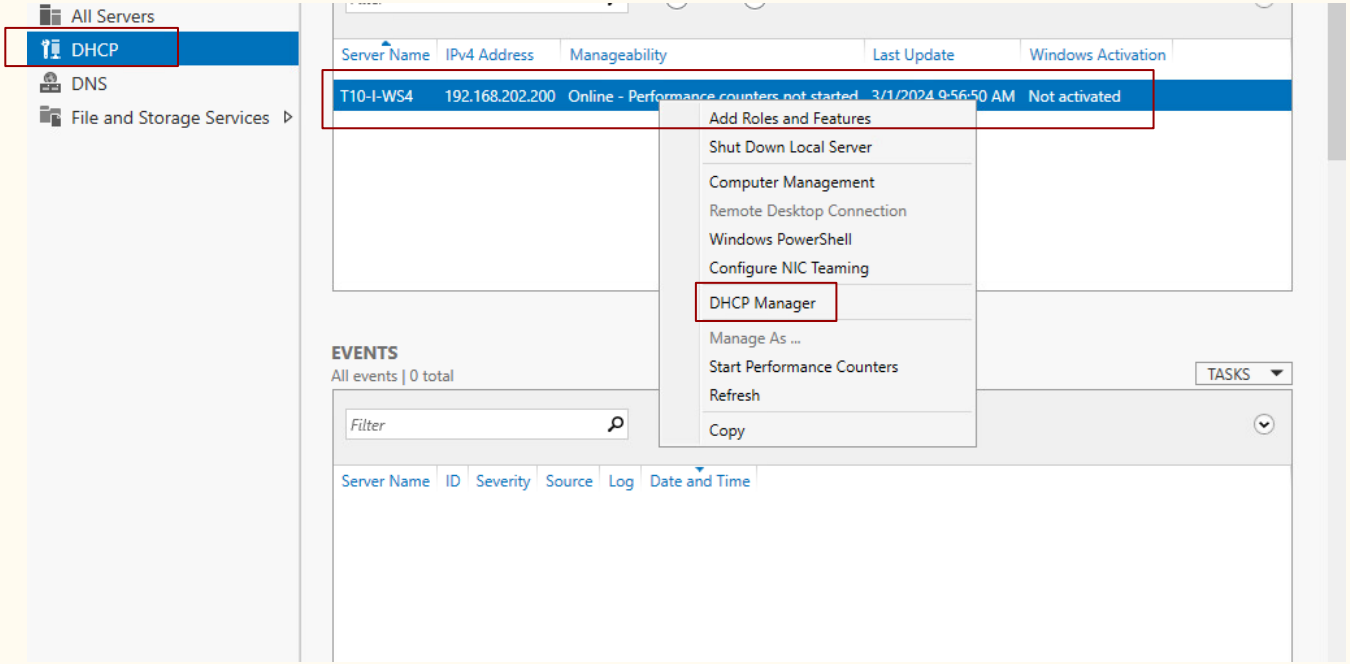
Post-deployment configurations

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



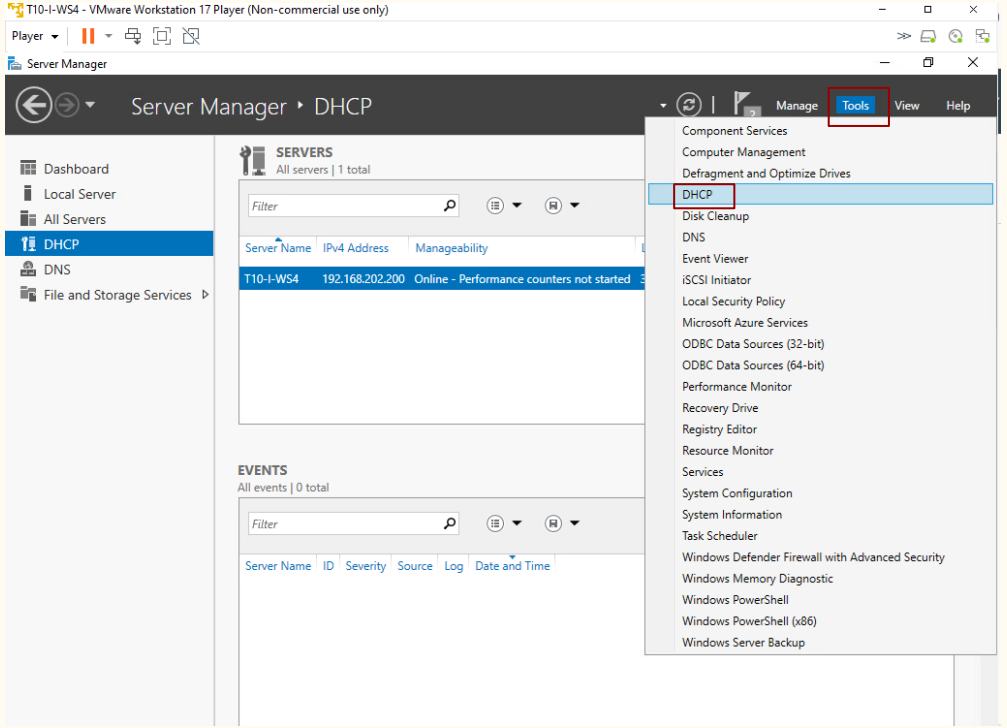
DHCP configuration

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.



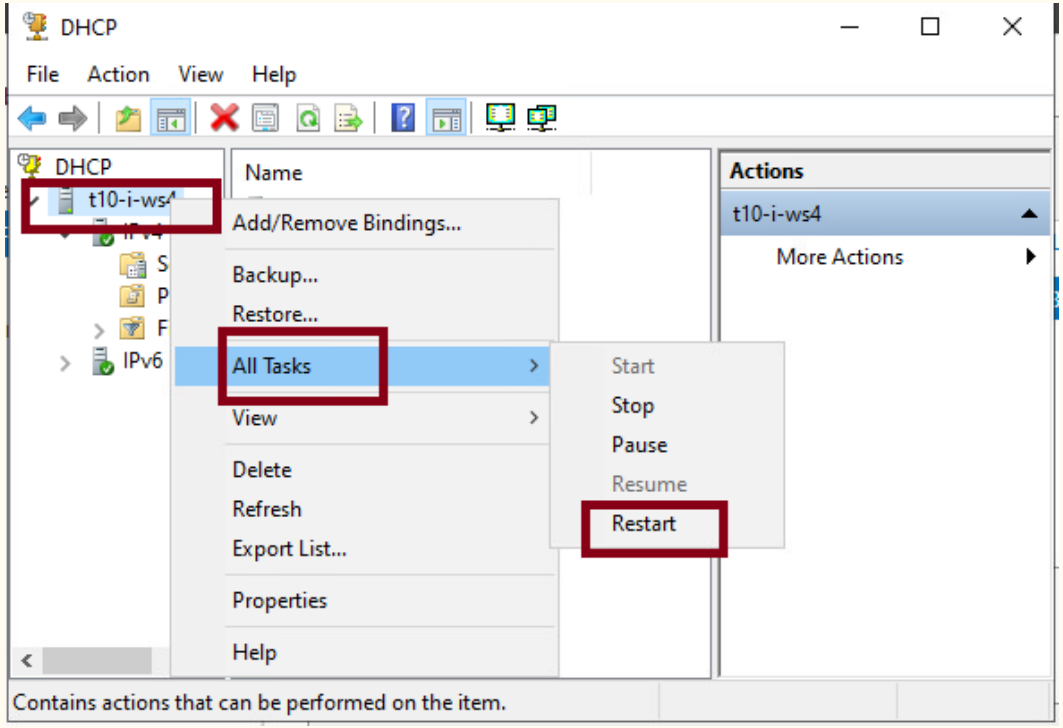
DHCP configuration.

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.



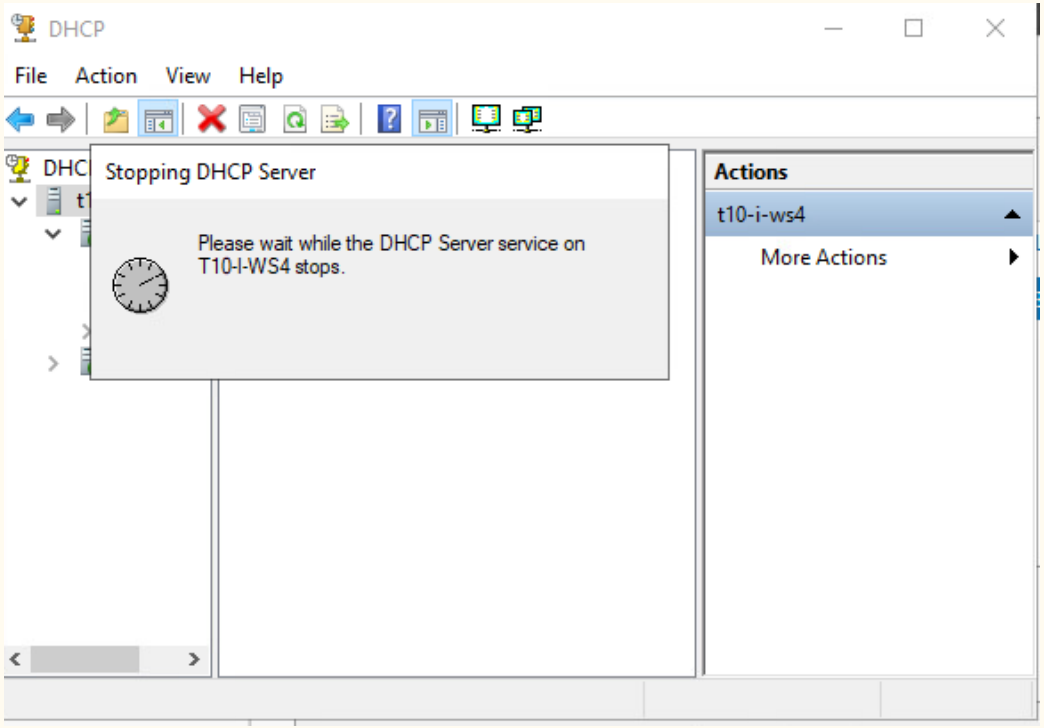
DHCP configuration.

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



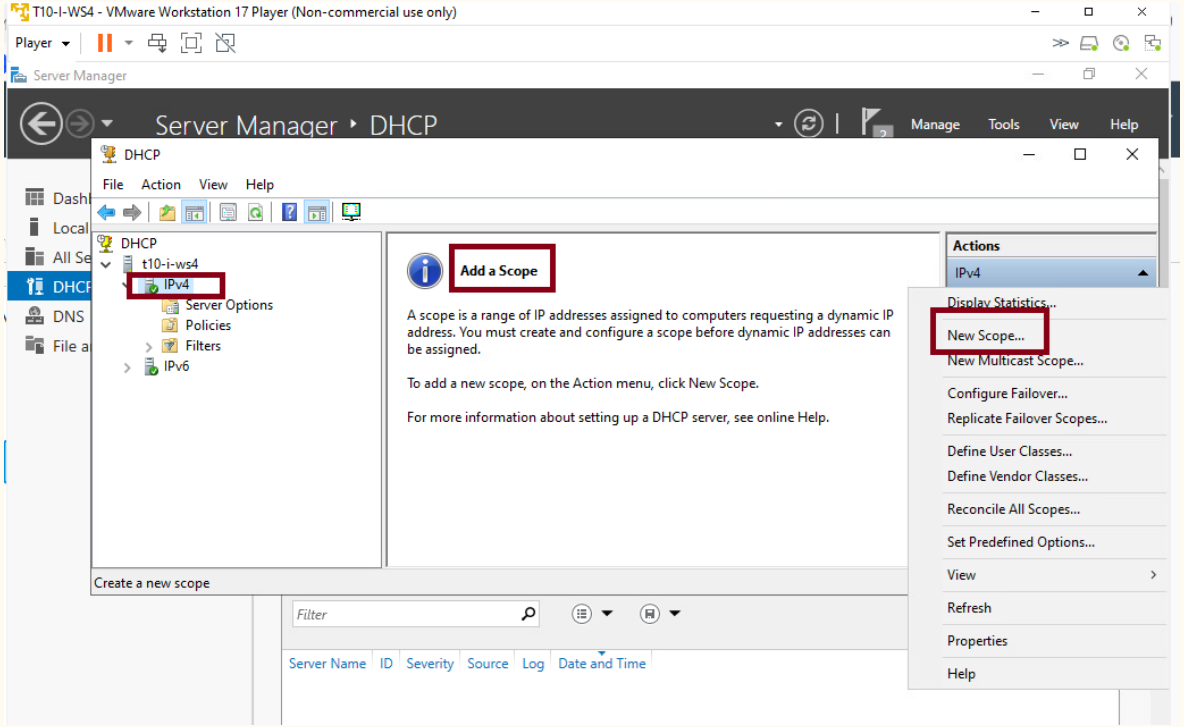
DHCP configuration.

The server will restart to get all the last updates.



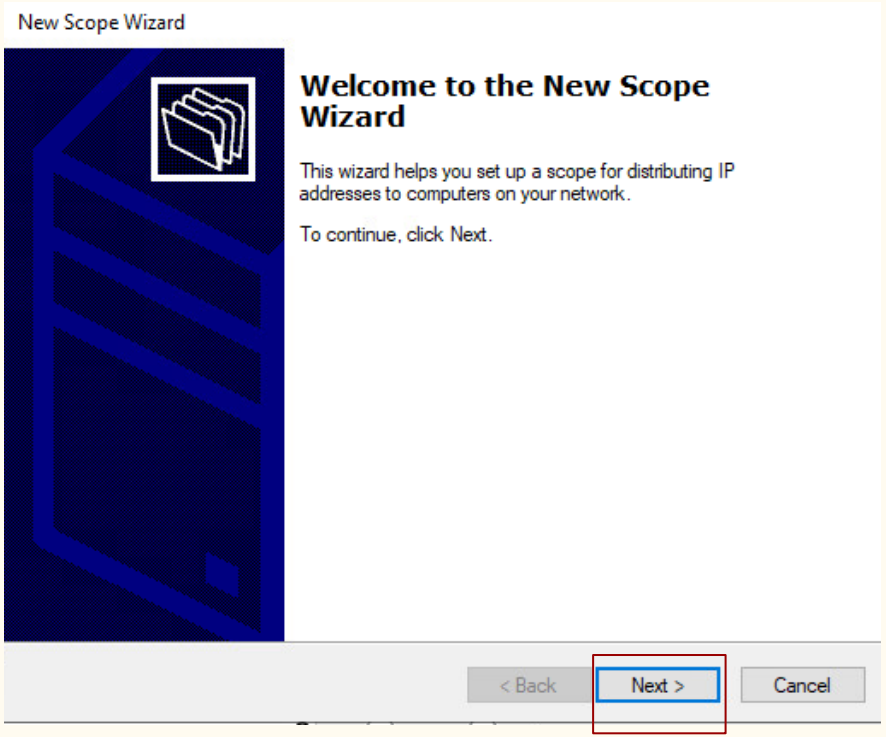
DHCP configuration. Add scopes.

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.



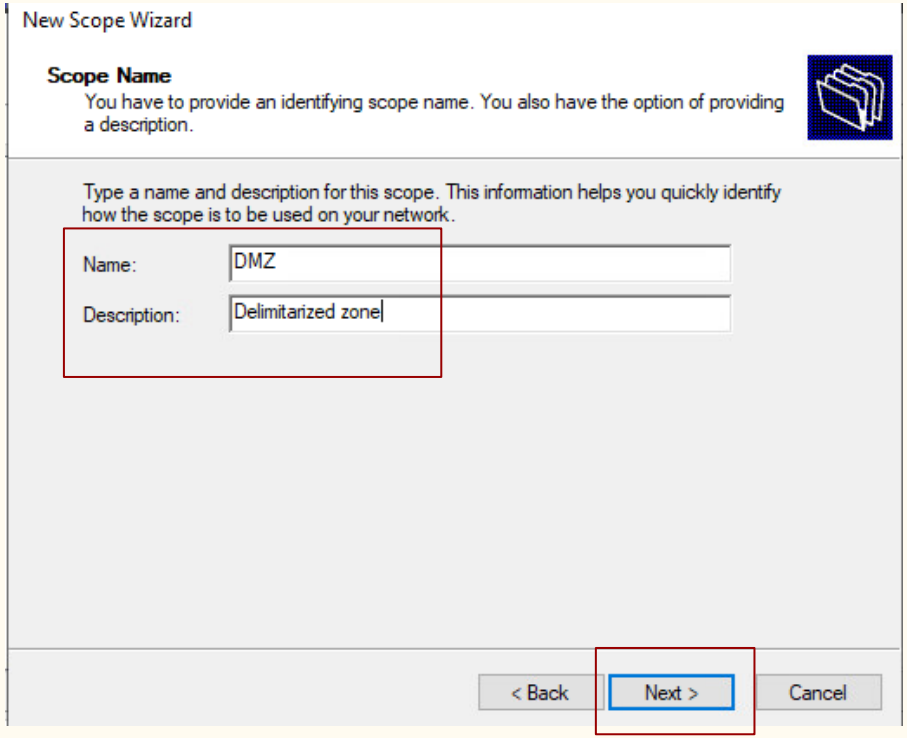
DHCP configuration. Add scopes.

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



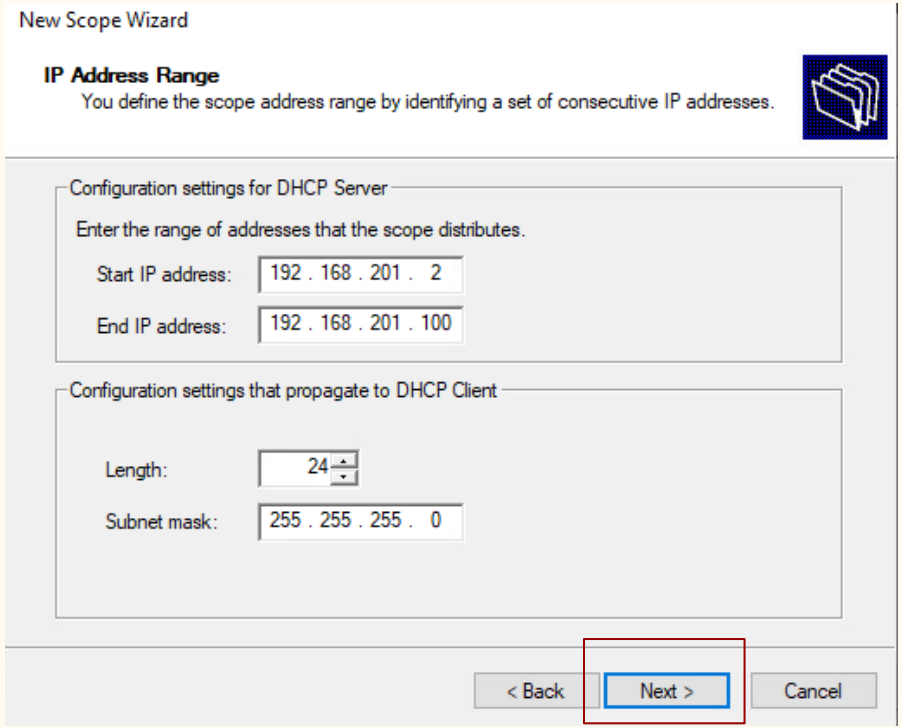
DHCP configuration. Add scopes.

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



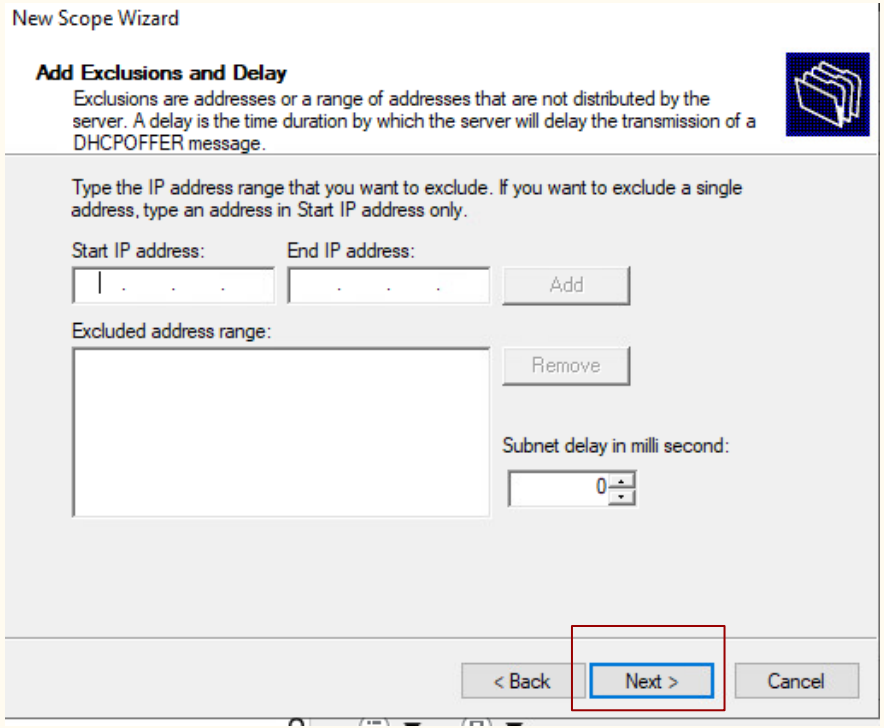
DHCP configuration. Add scopes.

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



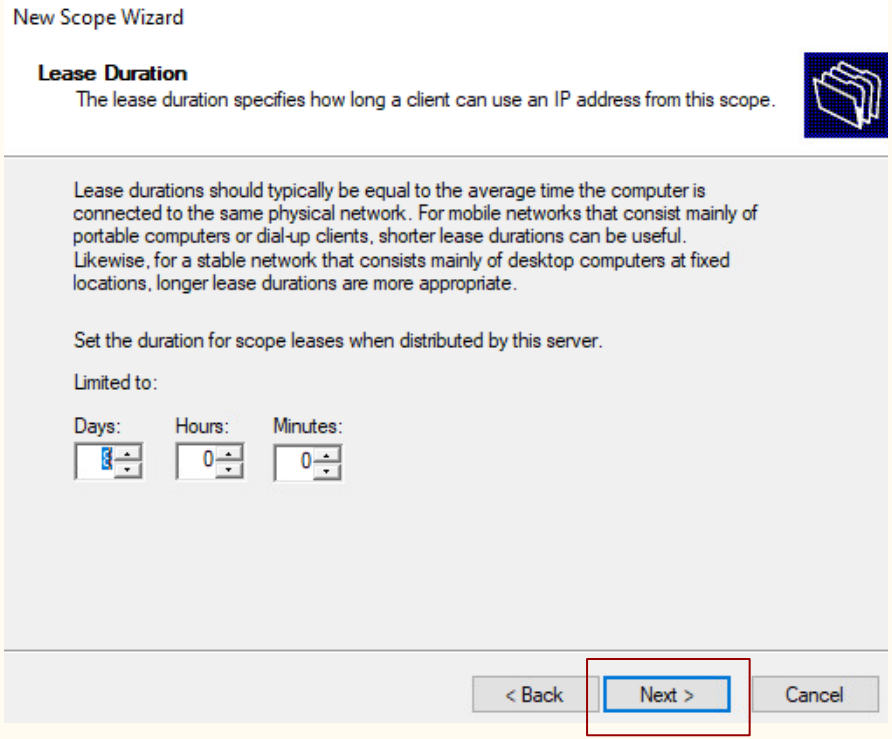
DHCP configuration. Add scopes.

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



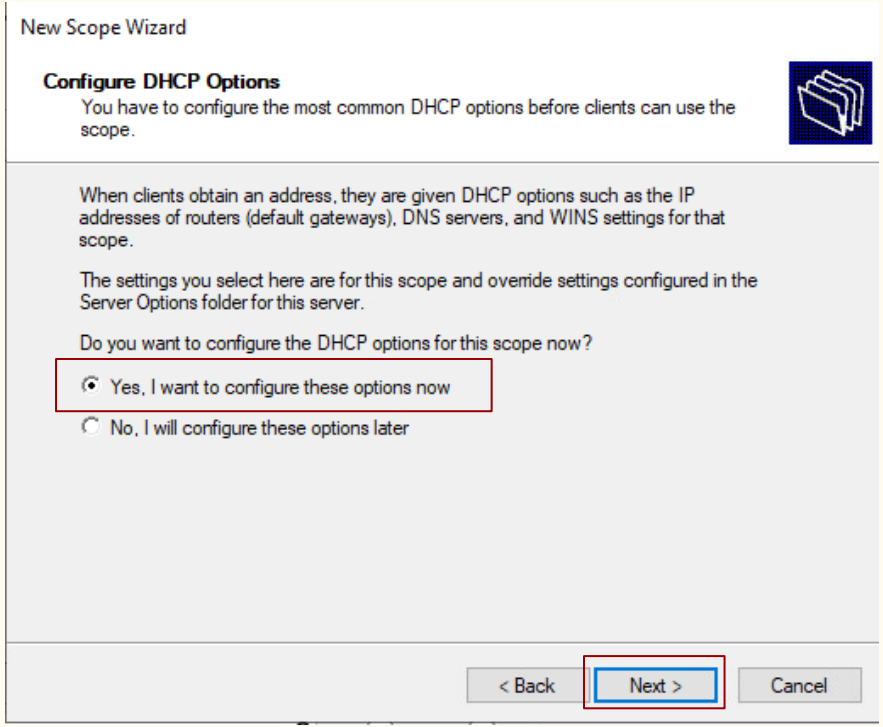
DHCP configuration. Add scopes.

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



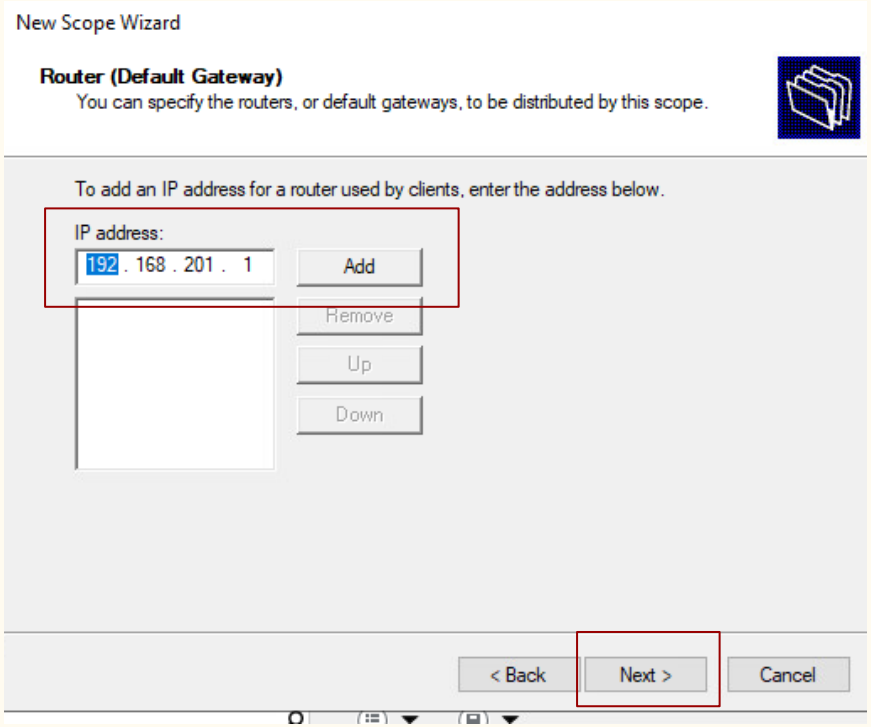
DHCP configuration. Add scopes.

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



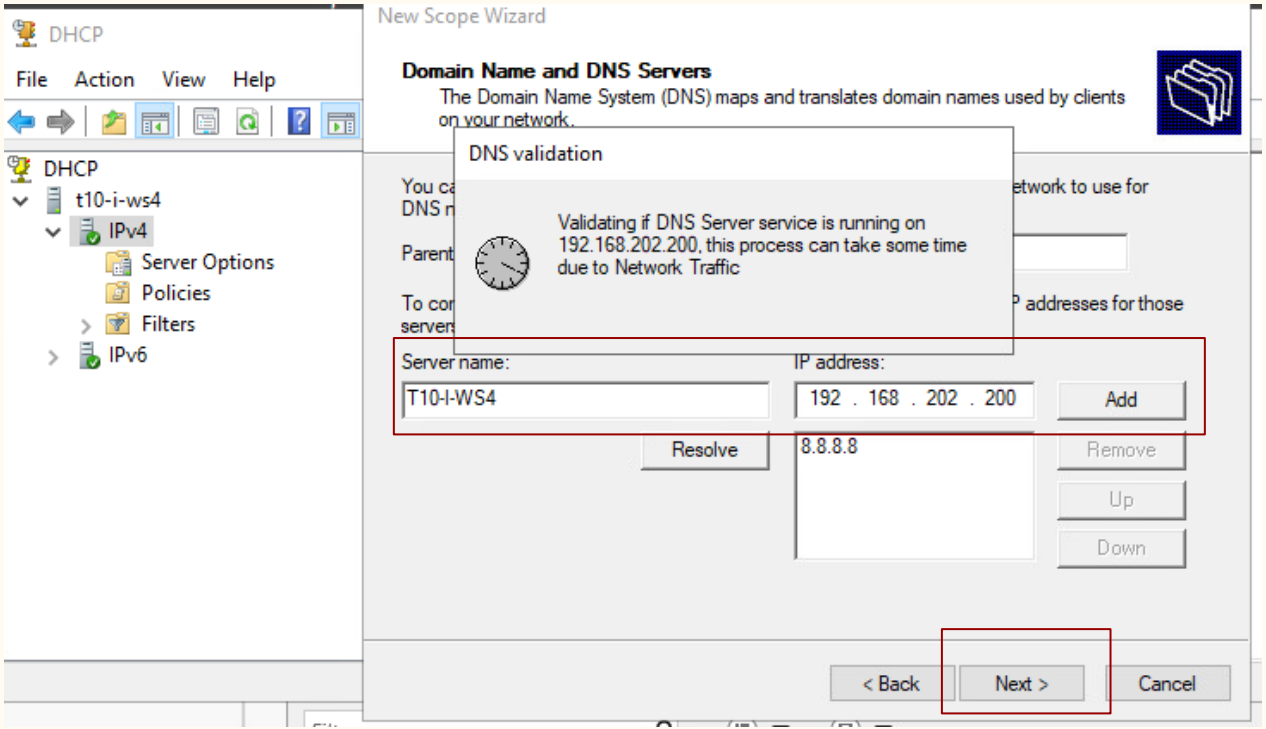
DHCP configuration. Add scopes.

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



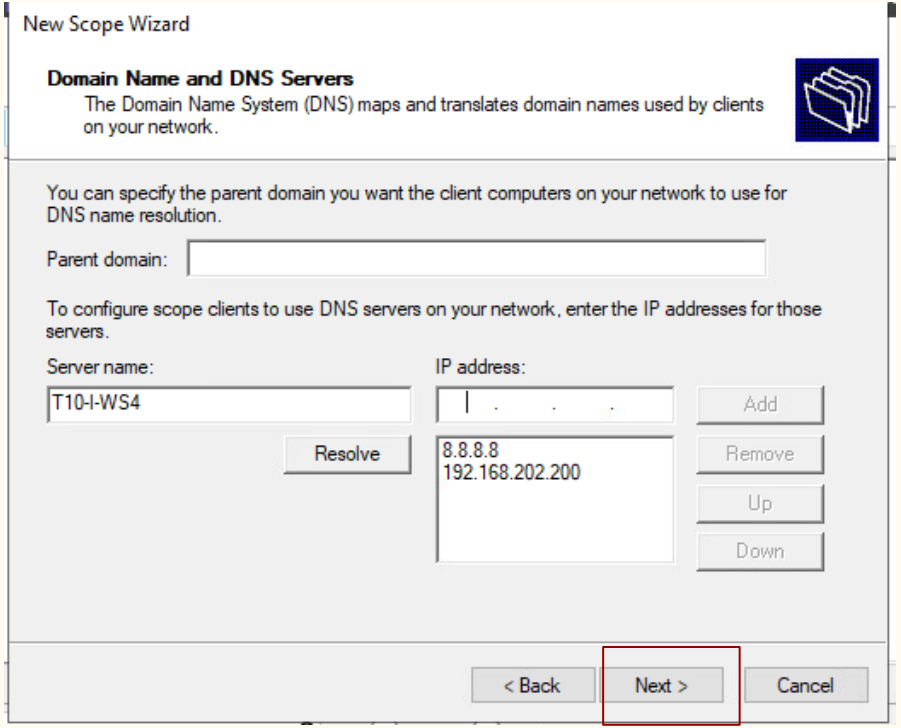
DHCP configuration. Add scopes.

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.



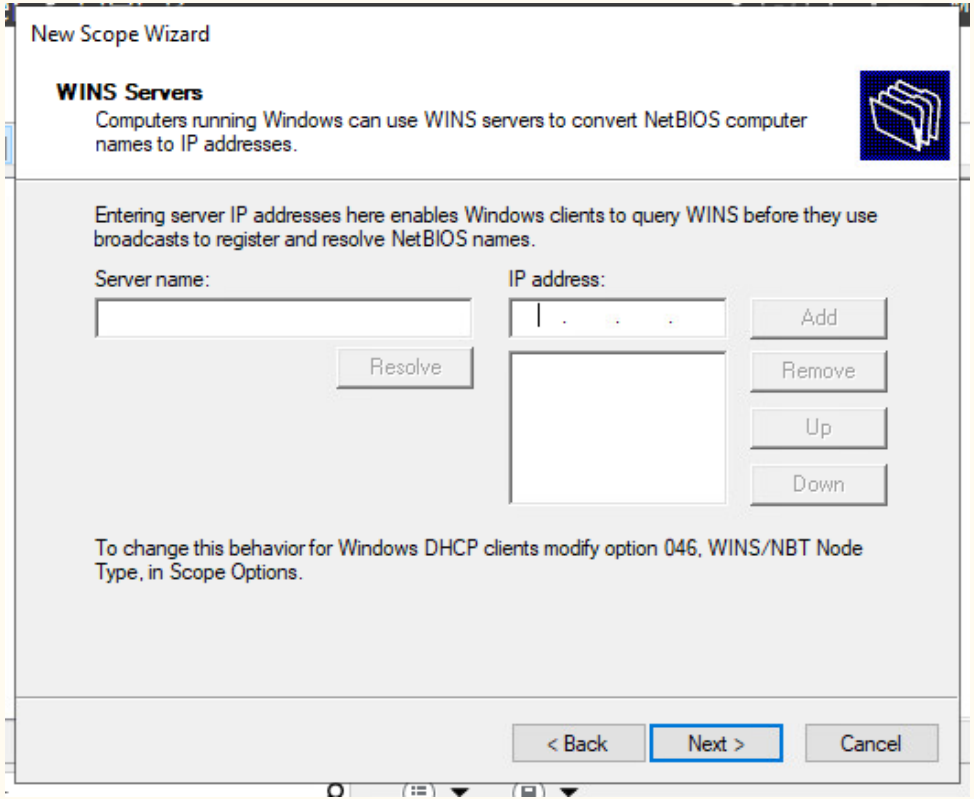
DHCP configuration. Add scopes.

After validation you can select next.



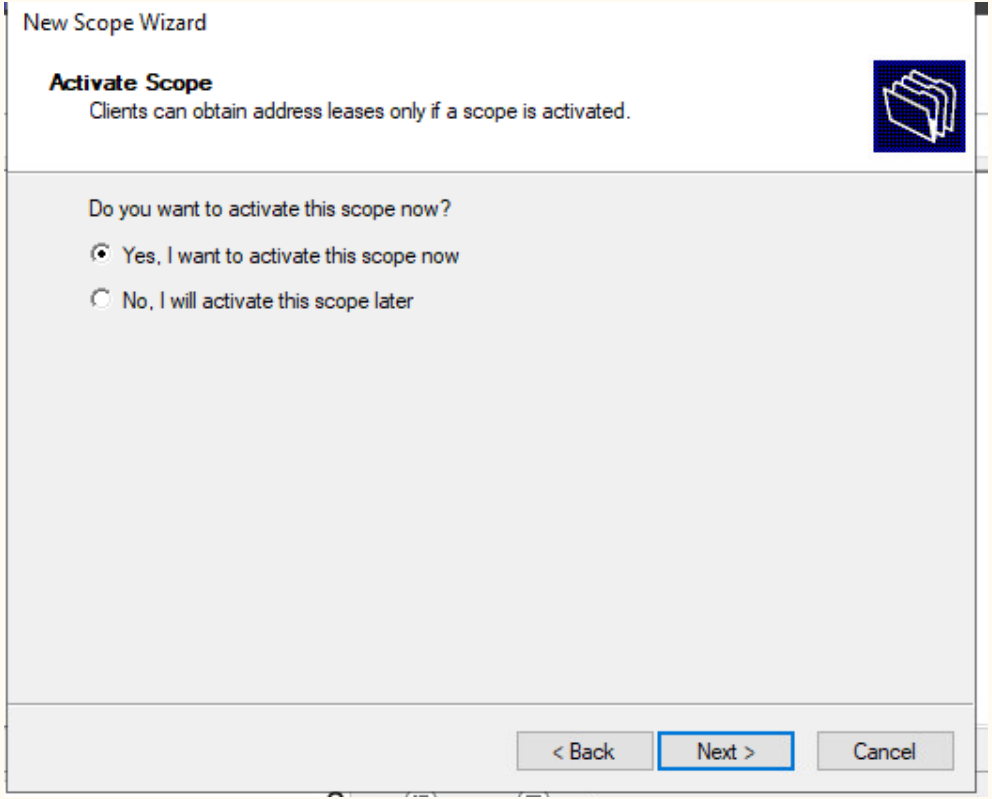
DHCP configuration. Add scopes.

In this case we will not configure WINS servers.



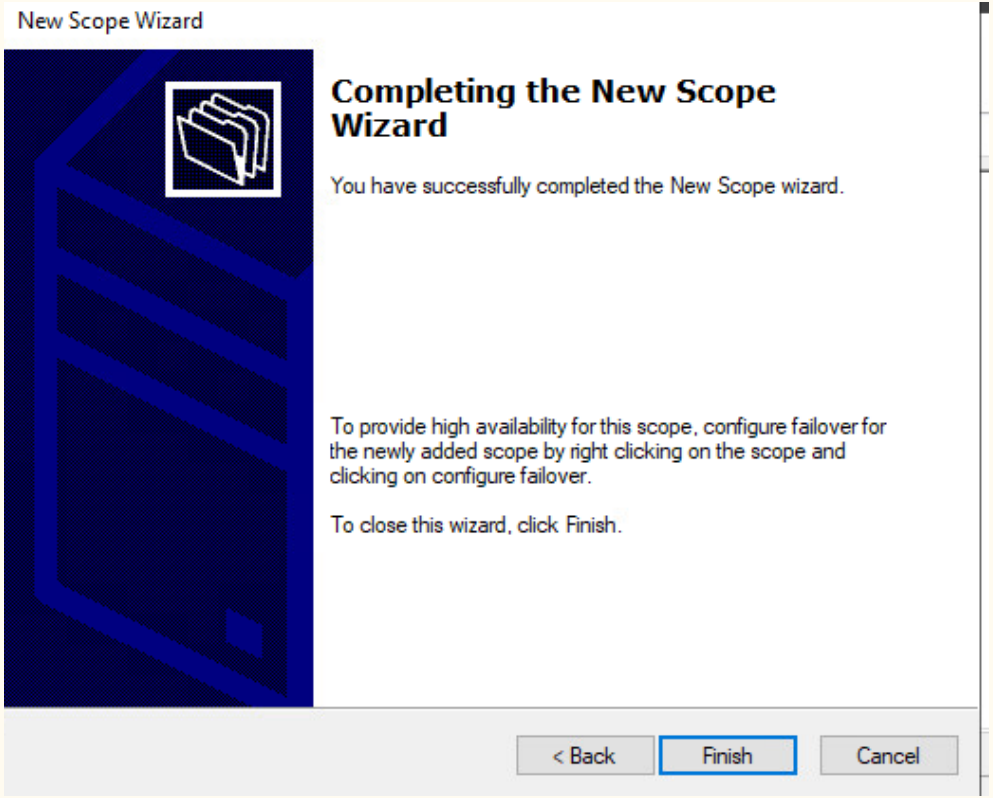
DHCP configuration. Add scopes.

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.



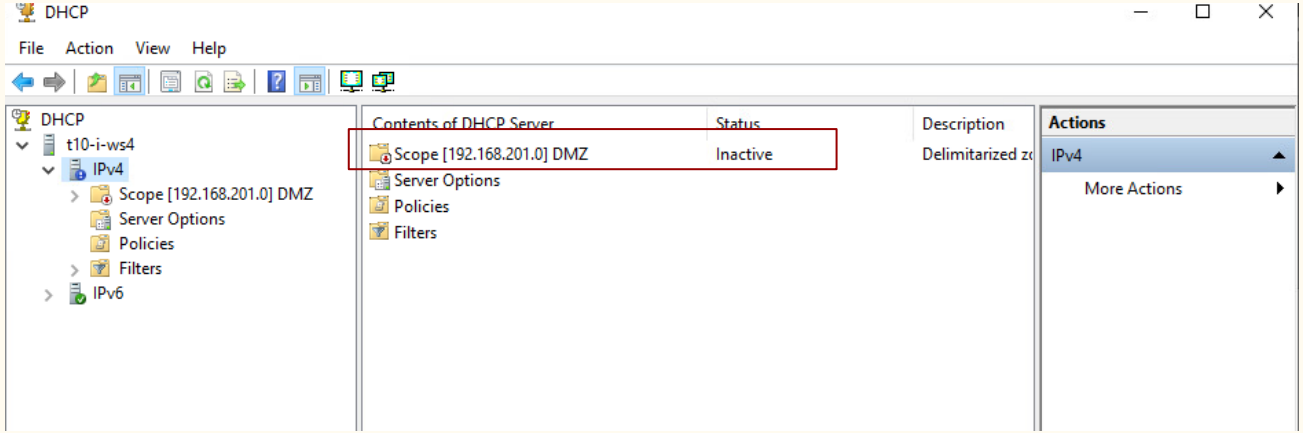
DHCP configuration. Add scopes.

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



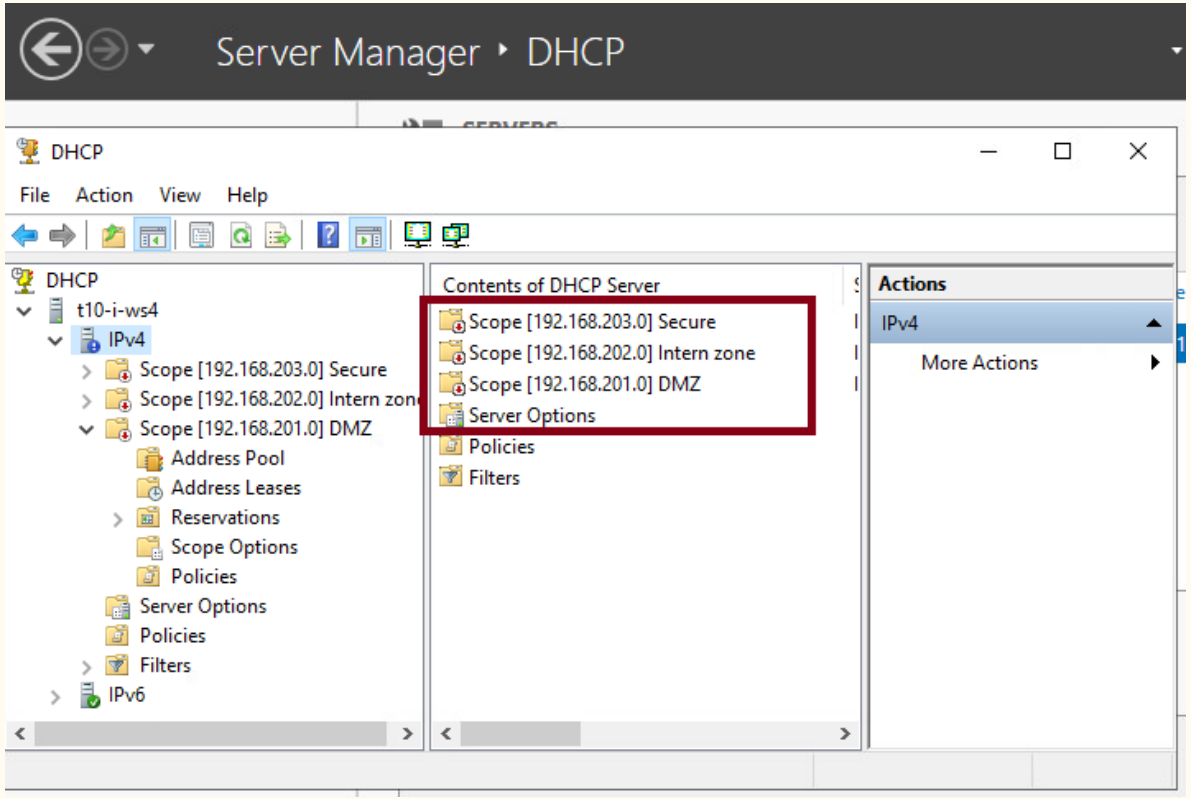
DHCP configuration. Add scopes.

The first scope will appears 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.



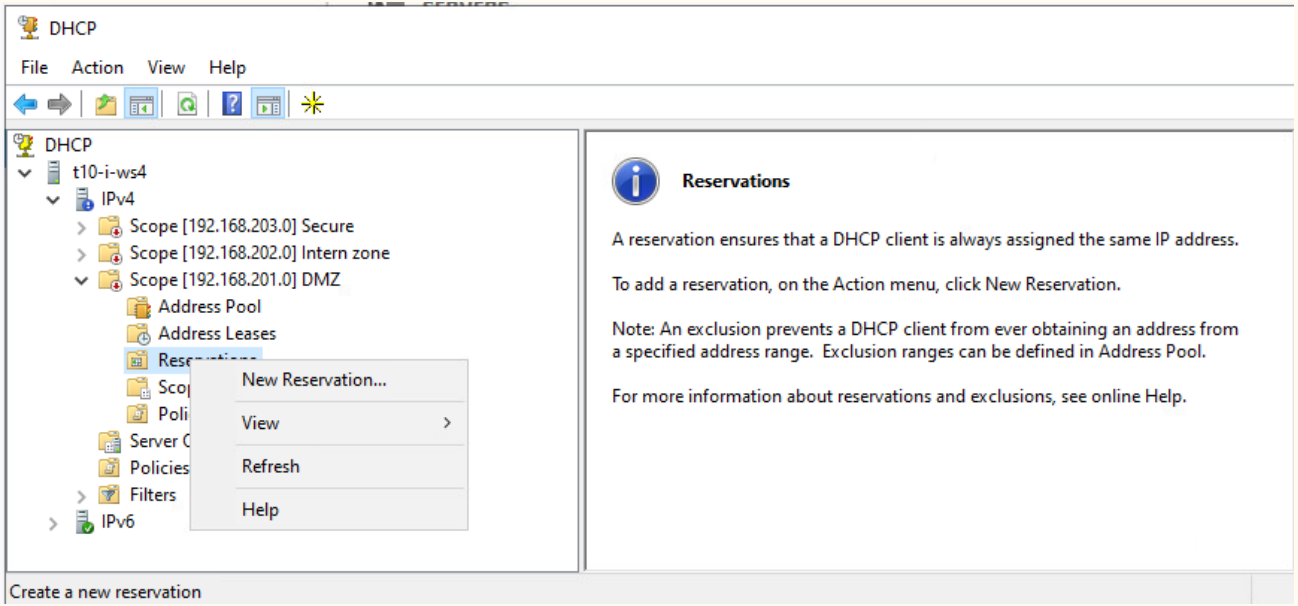
DHCP configuration. Add scopes.

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



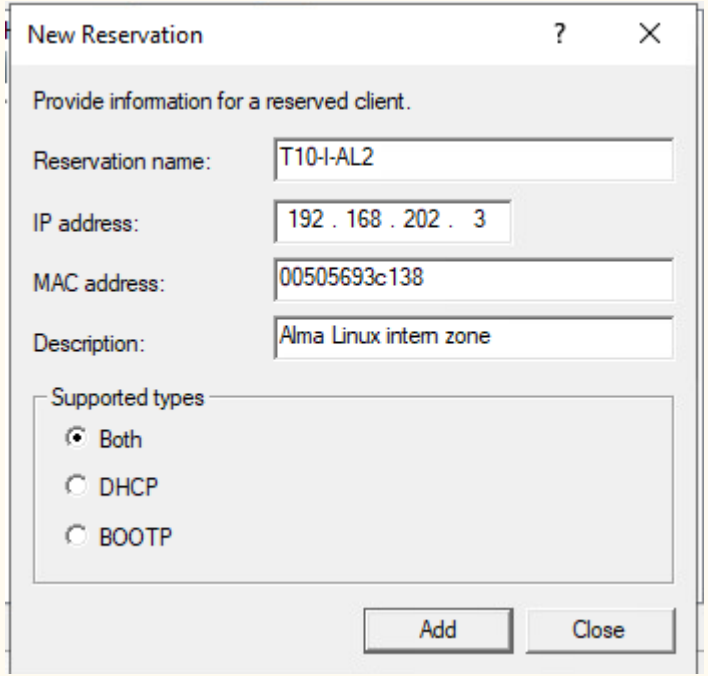
DHCP configuration. Add sticky addresses for our servers.

It is not secure and impractical that our servers lease differents 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.



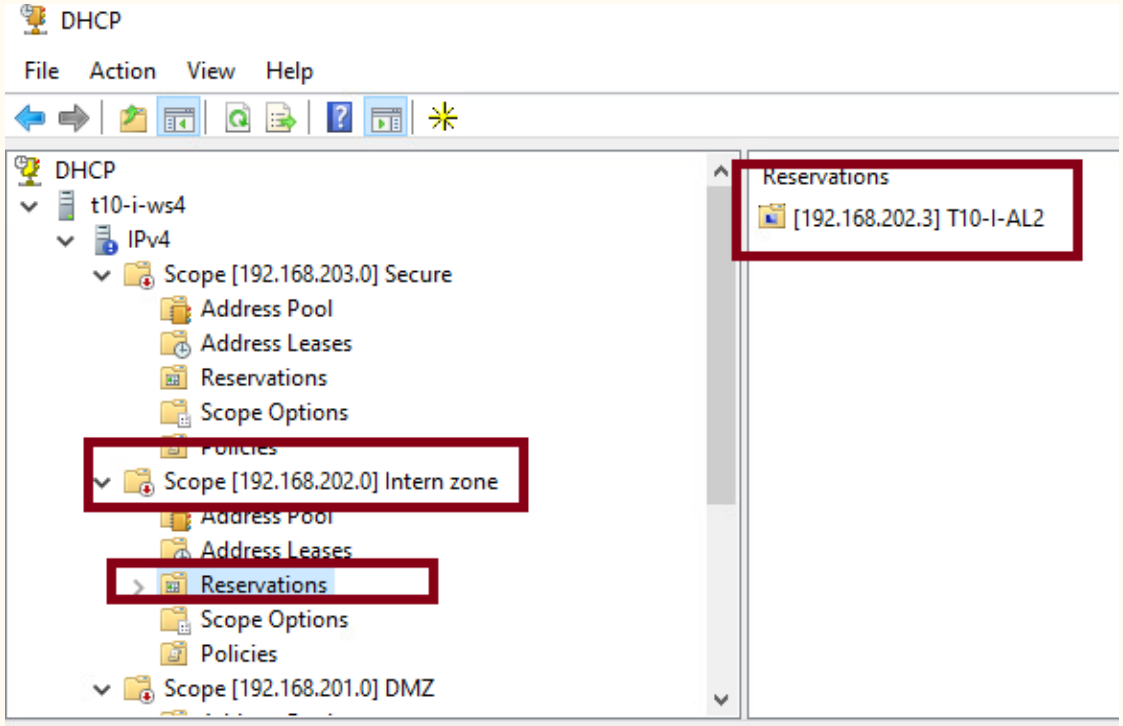
DHCP configuration. Add sticky addresses for our servers.

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 were you can add more reservations for your entire scope.



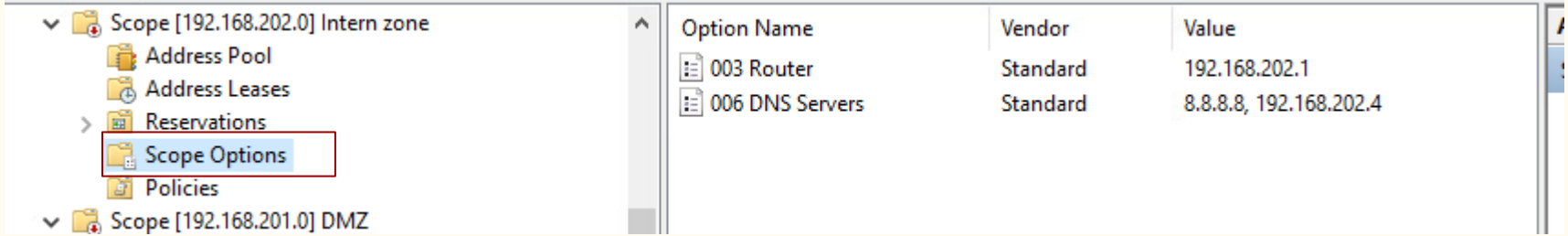
DHCP configuration. Add sticky addresses for our servers.

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.



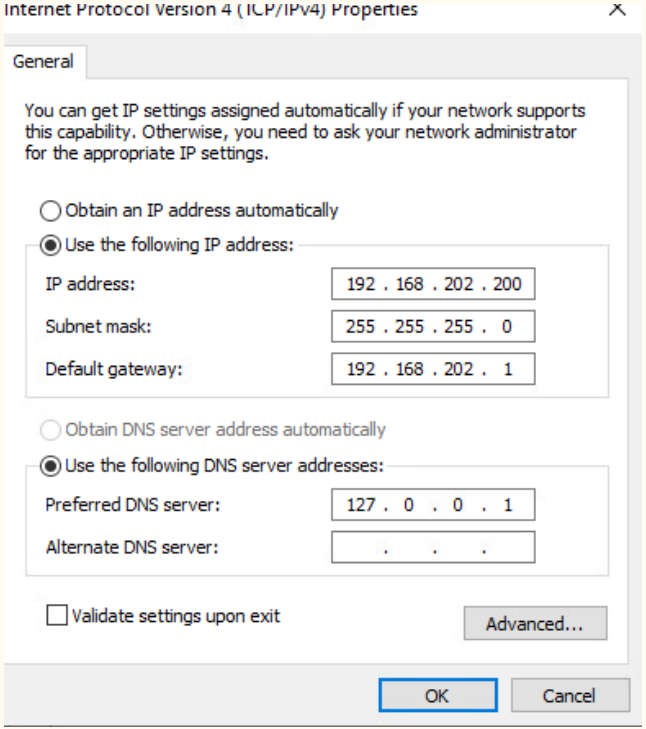
DHCP configuration. Scope options.

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.



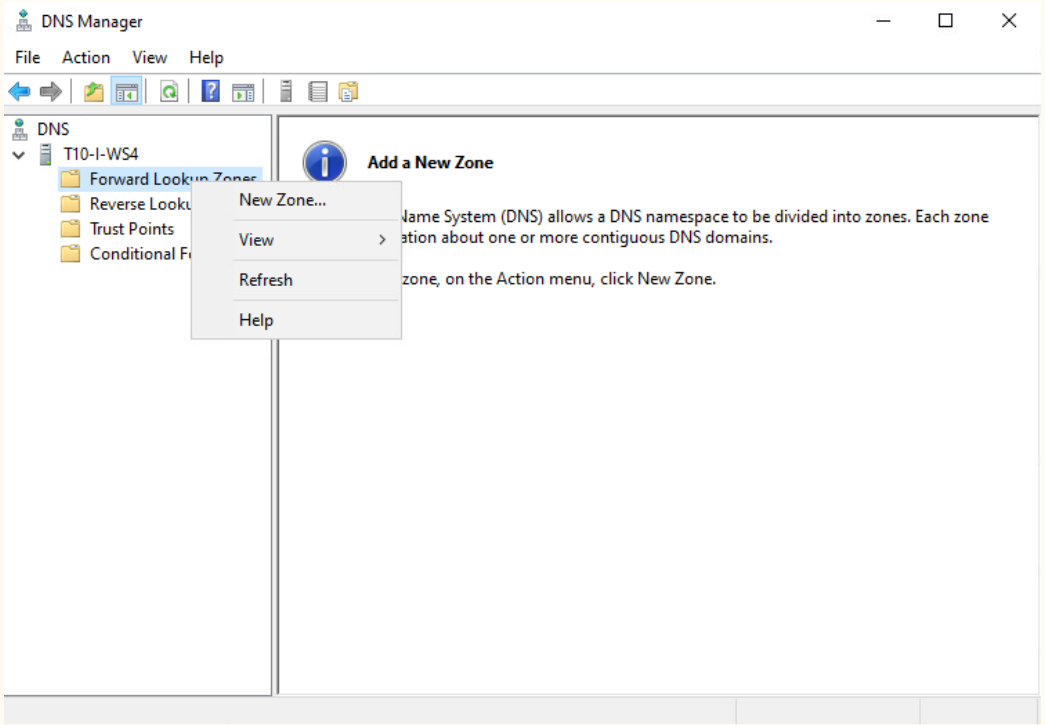
DNS Configuration on DNS server.

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.

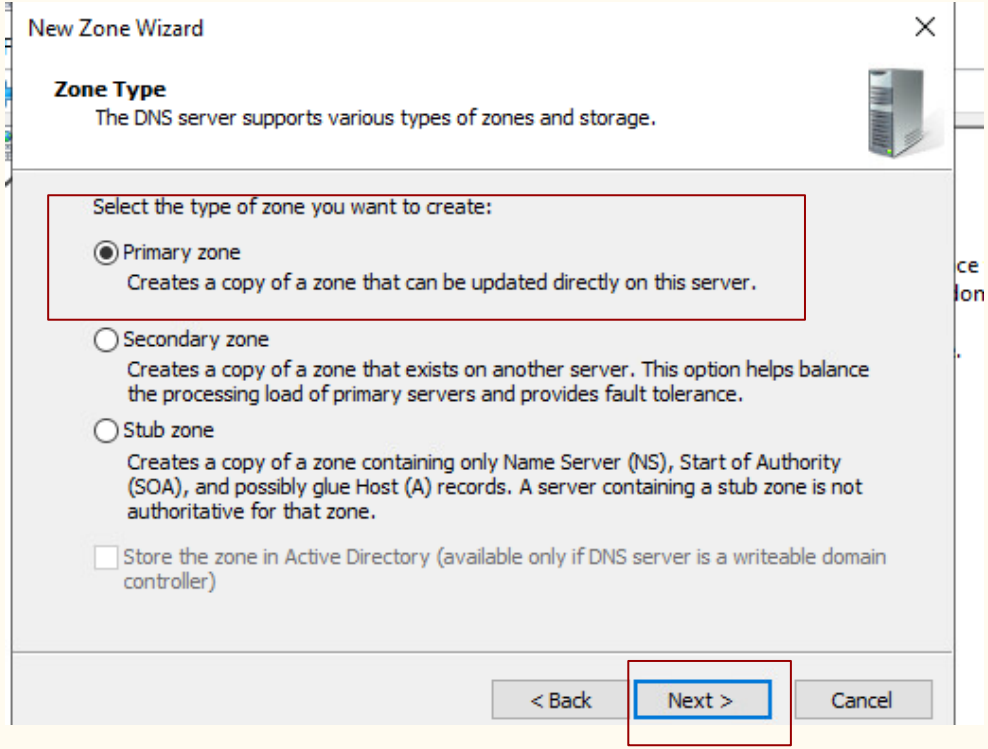


DNS configurations.

This interface will guide us along the configuration process.

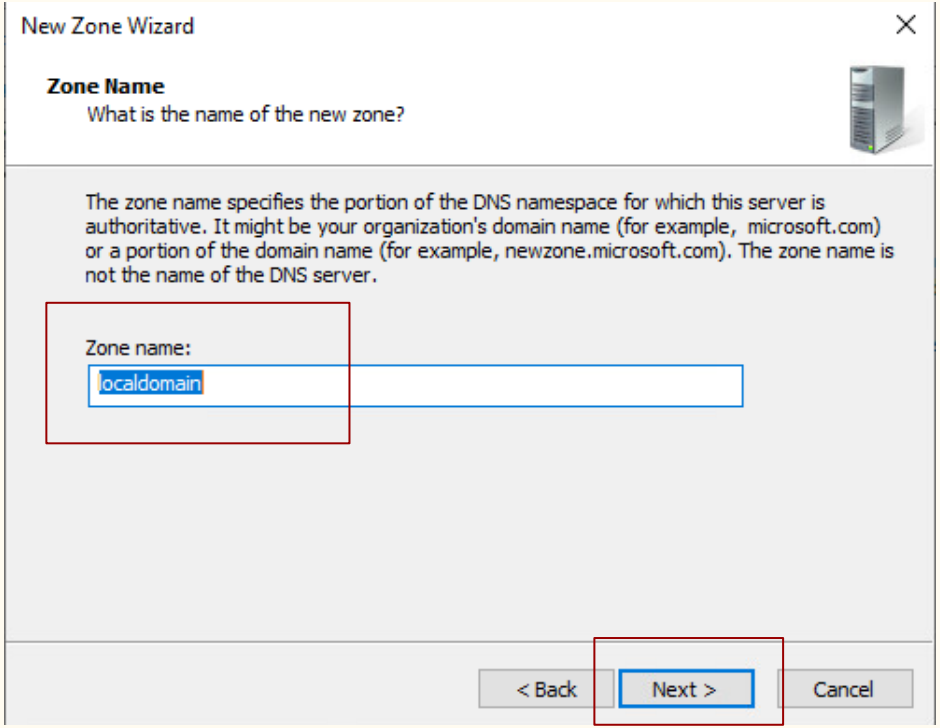
DNS configurations.

Select Primary zone in the first window and click next.



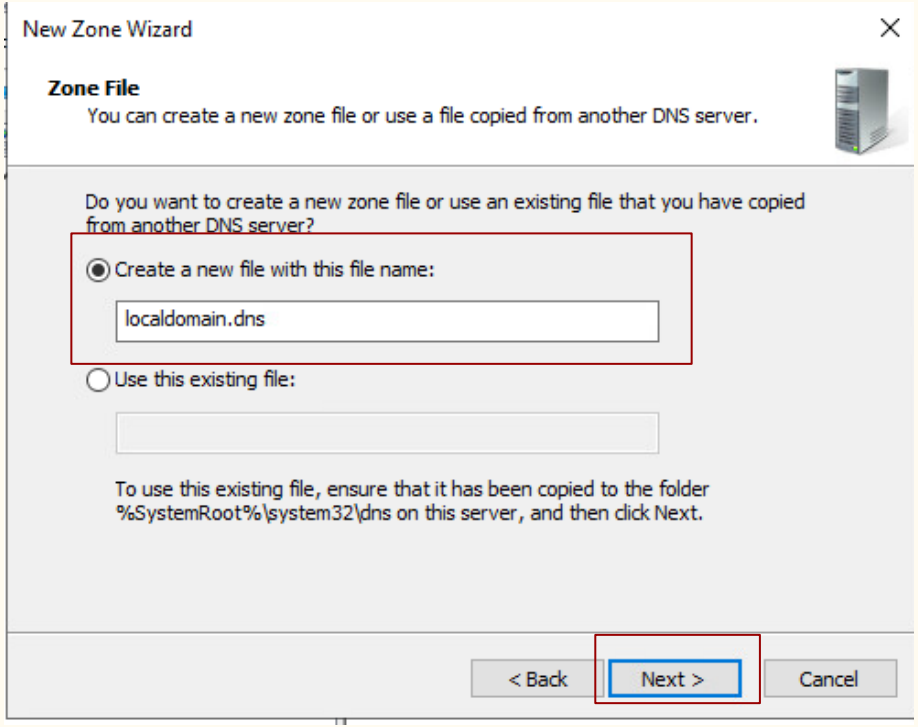
DNS configurations.

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



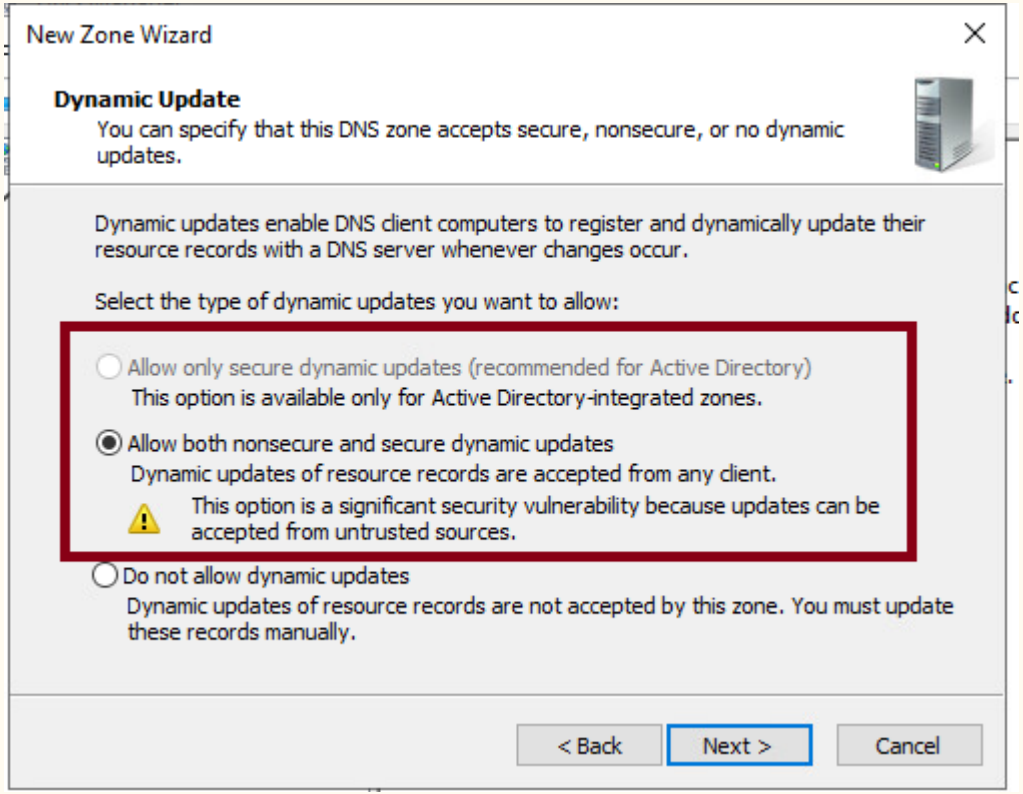
DNS configurations.

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



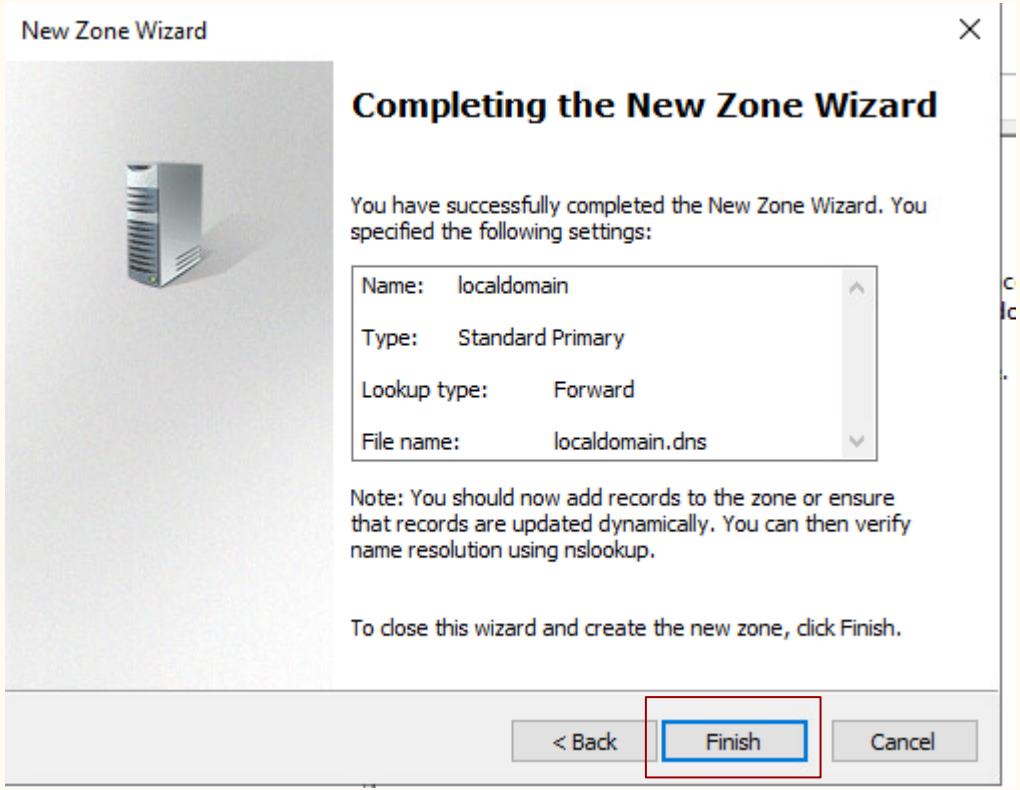
DNS configurations.

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...



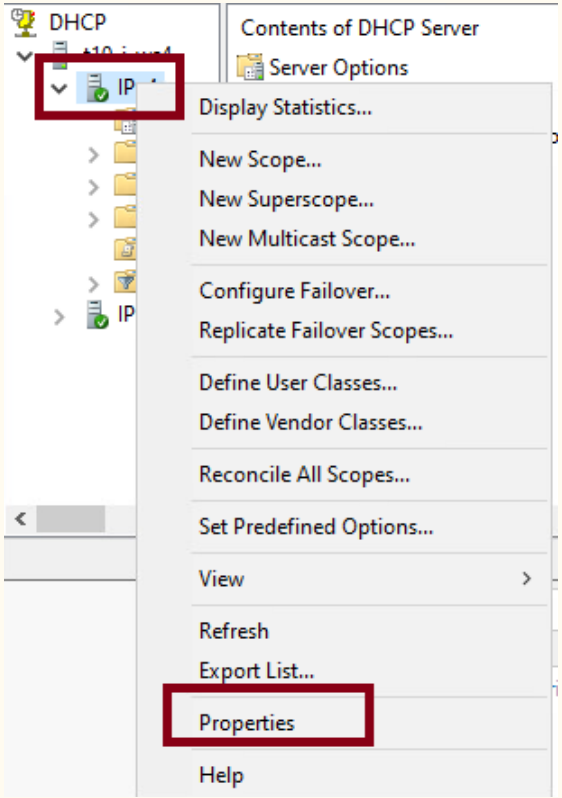
DNS configurations.

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



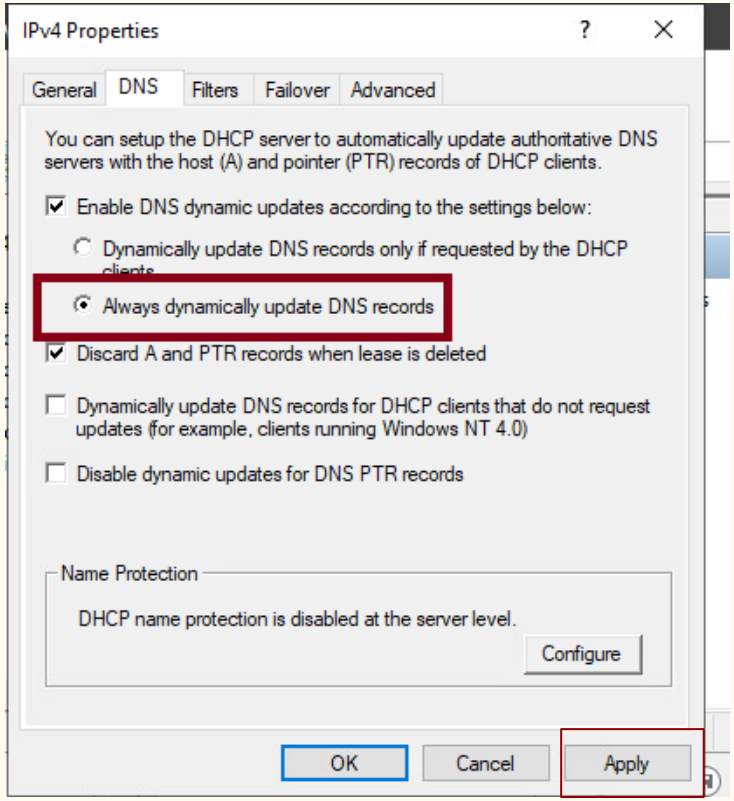
DNS configurations to allow dynamic updates from DHCP.

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



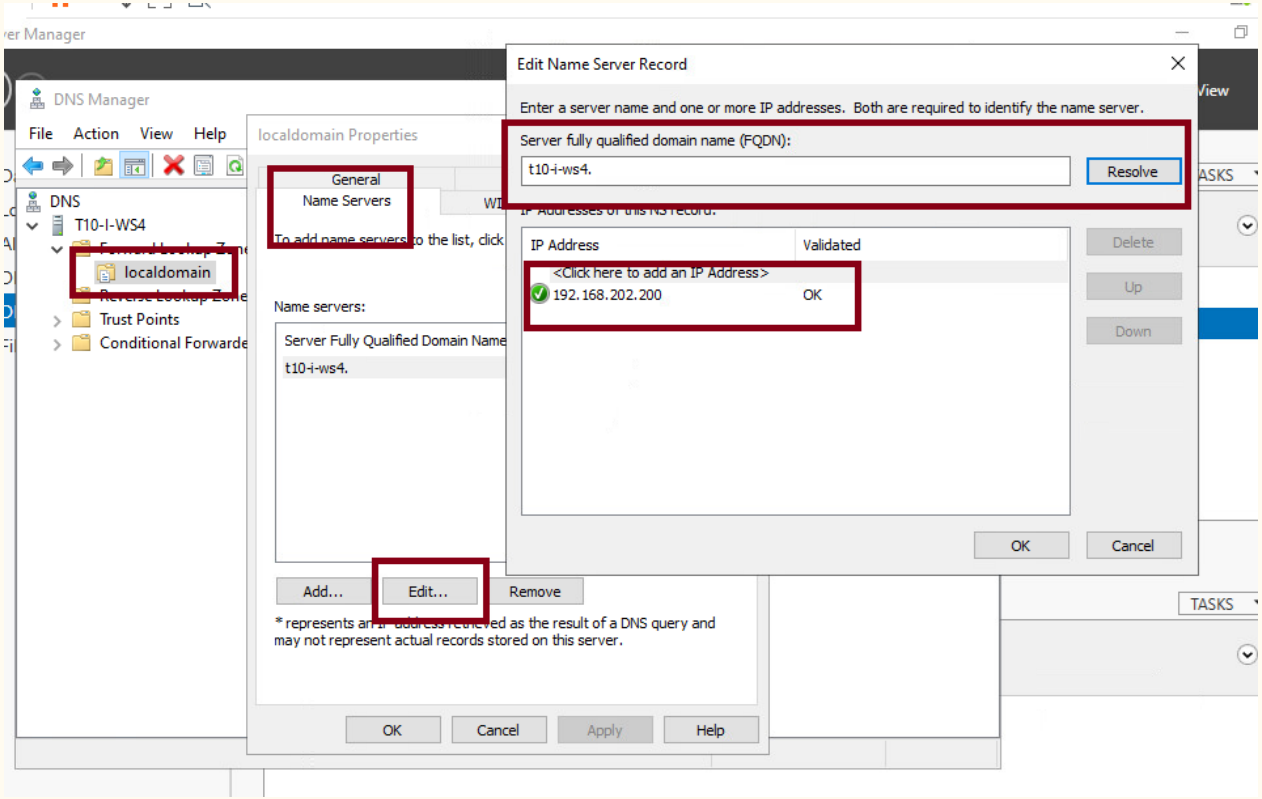
DNS configurations to allow dynamic updates from DHCP.

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.

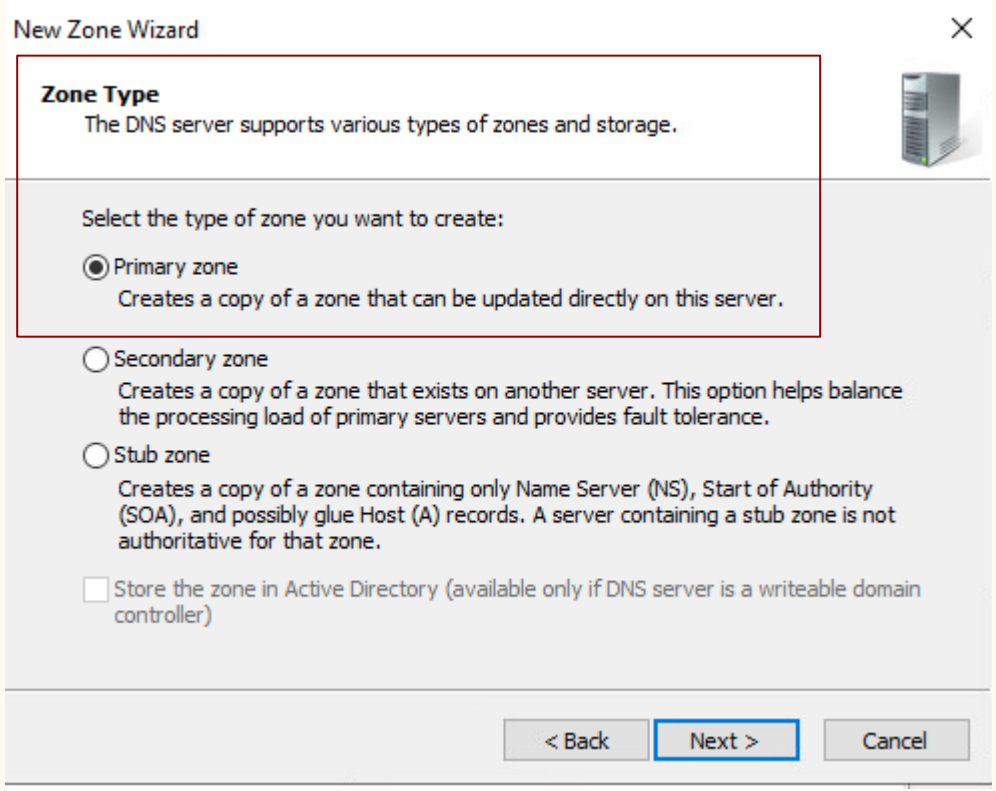


Reverse lookup zones.

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.

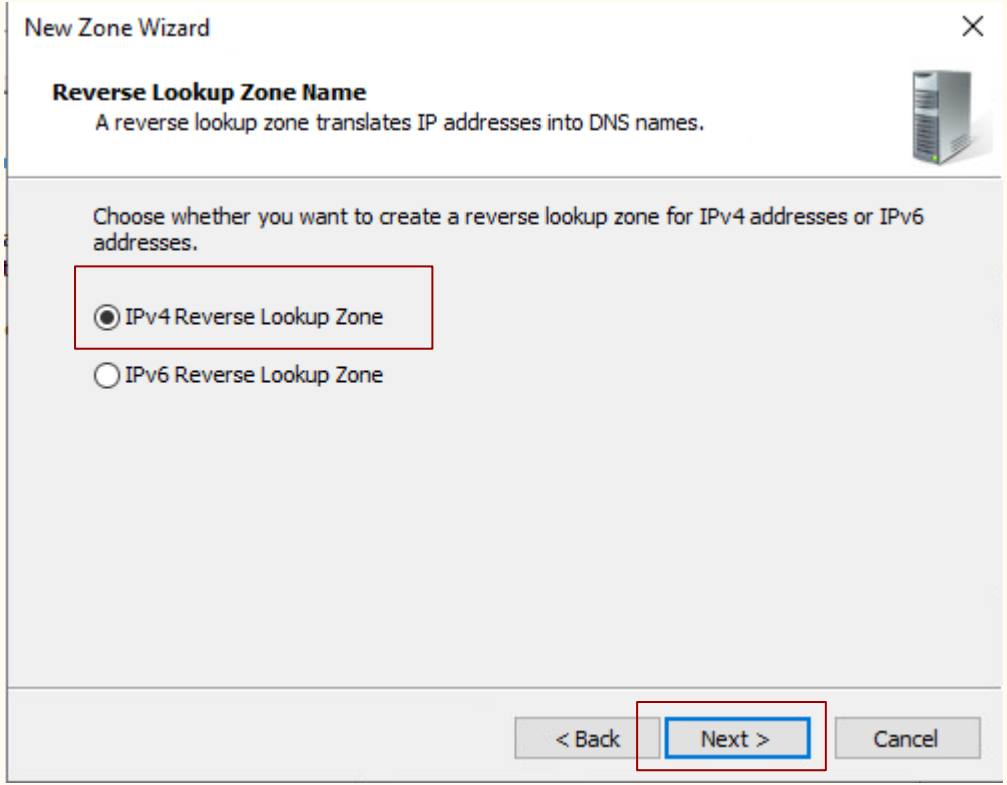
Reverse lookup zones.

Select Primary zone.



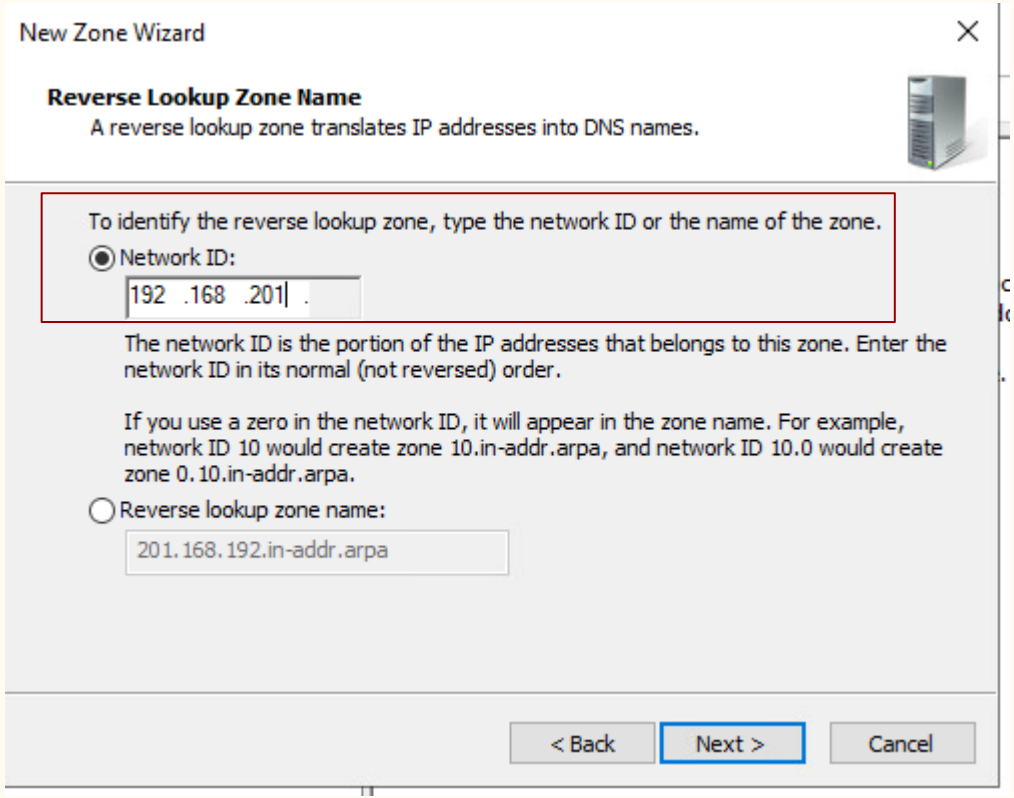
Reverse lookup zones.

Select IPv4 Reverse Lookup Zone. Click next.



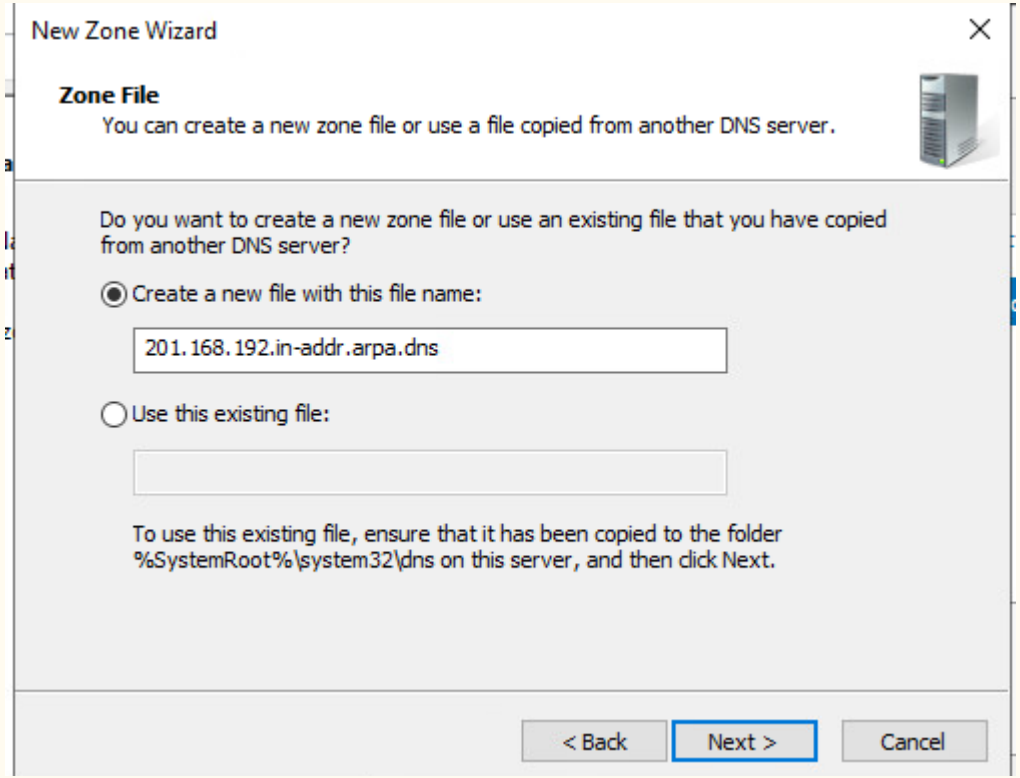
Reverse lookup zones.

Put the first 3 octet from the scope that you want to refers by this zone in network ID. Then click next.



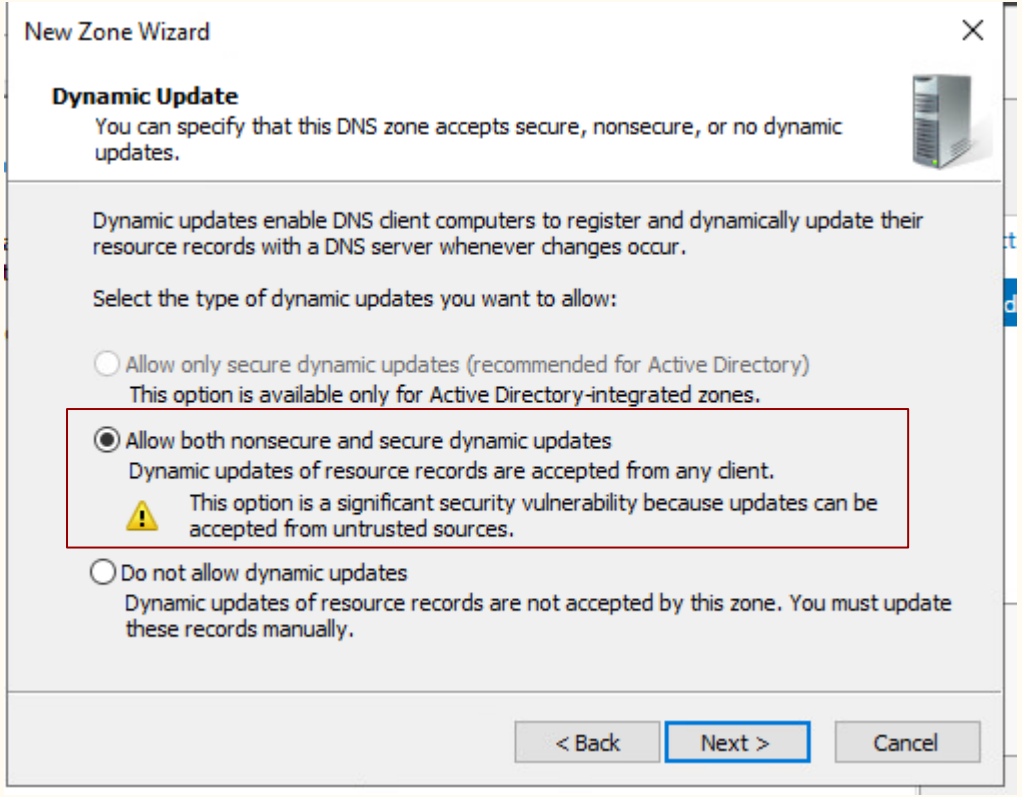
Reverse lookup zones.

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



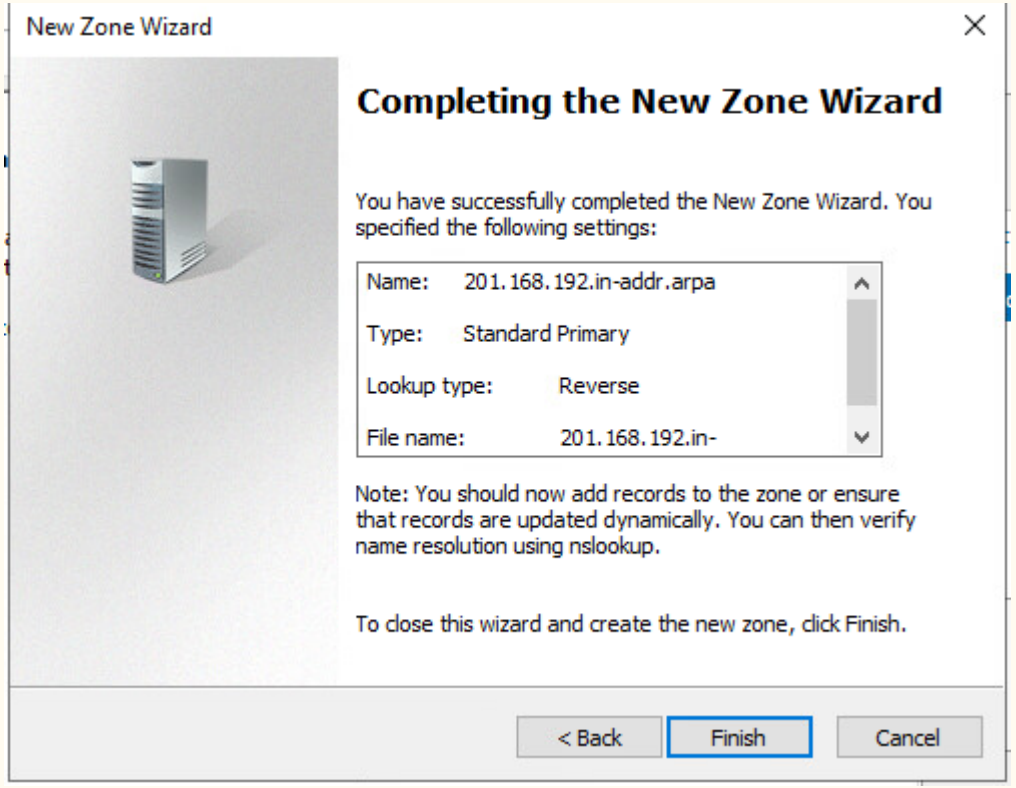
Reverse lookup zones.

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



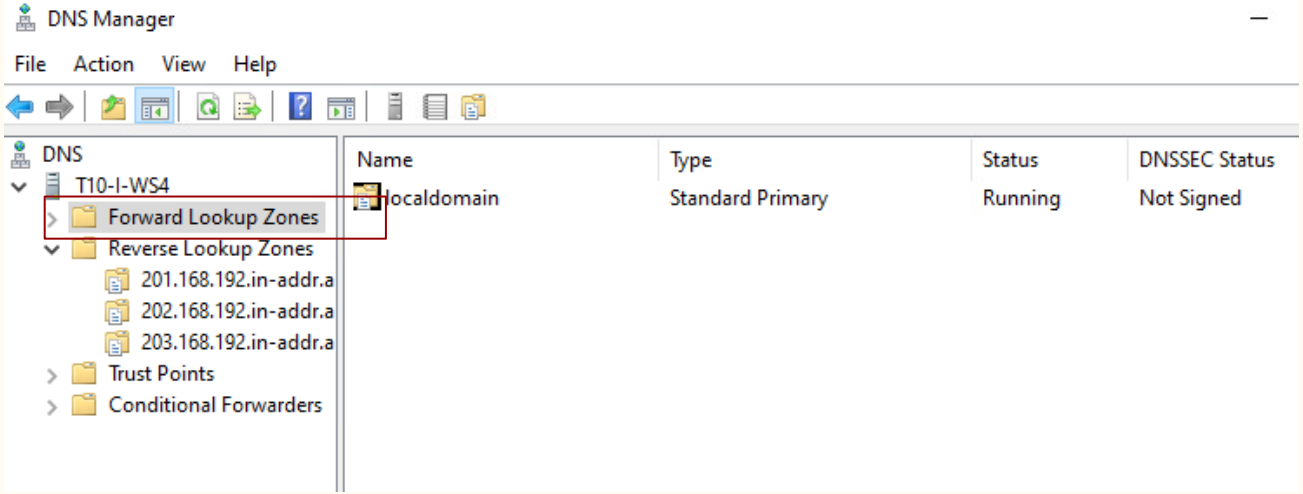
Reverse lookup zones.

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



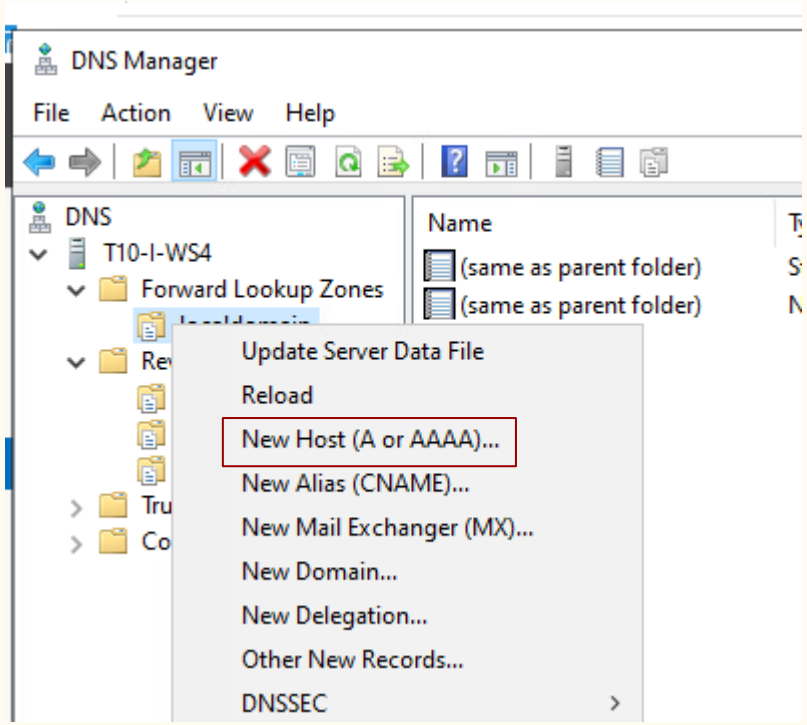
Check proper configurations.

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.



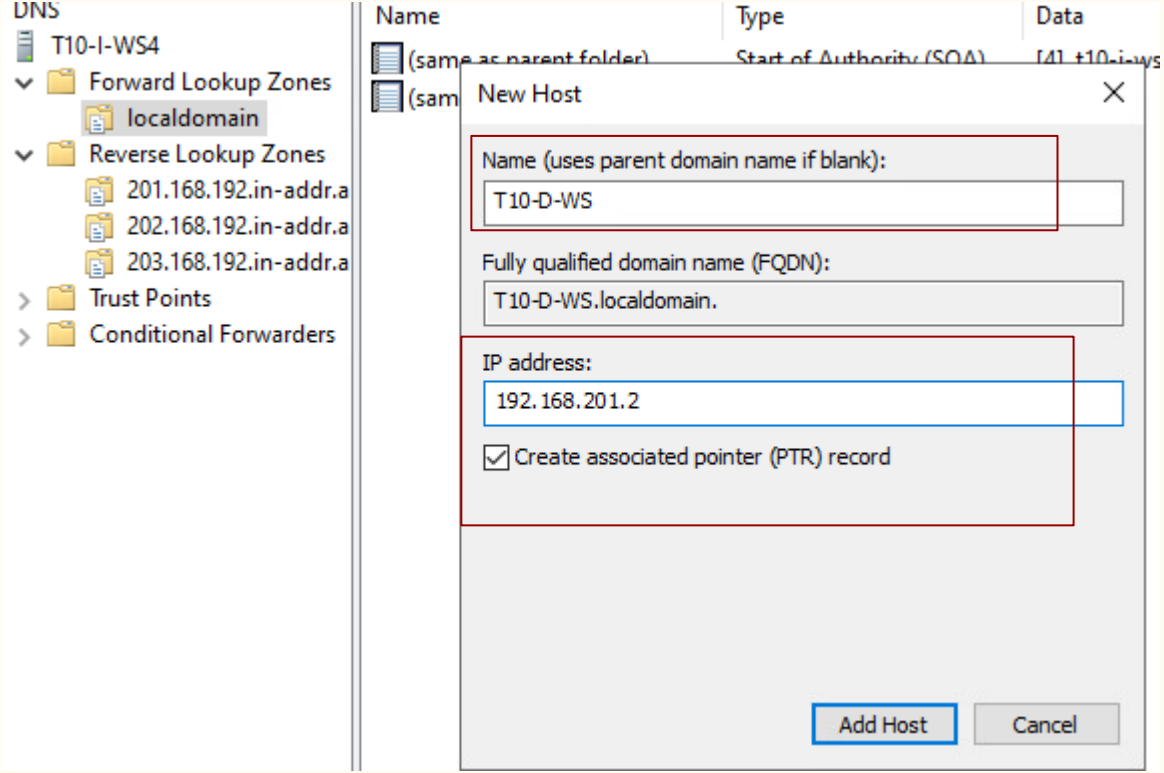
Check proper configurations.

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



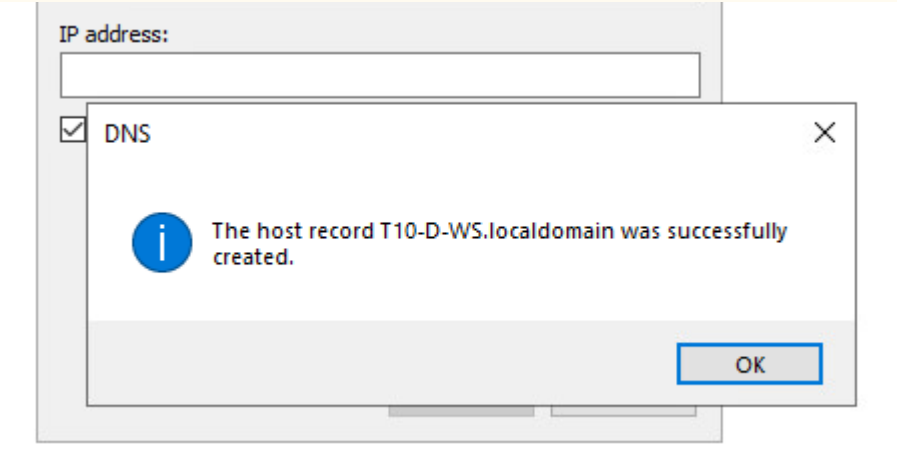
Check proper configurations.

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



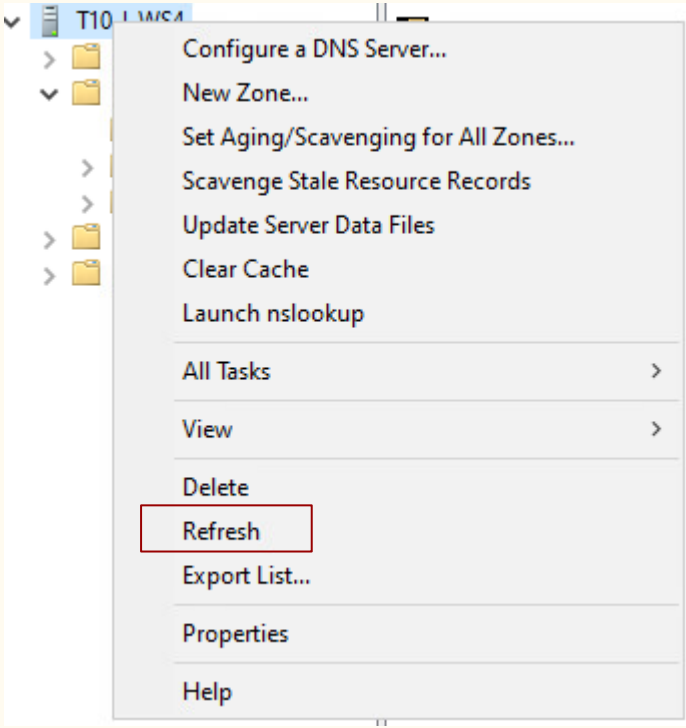
Check proper configurations.

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



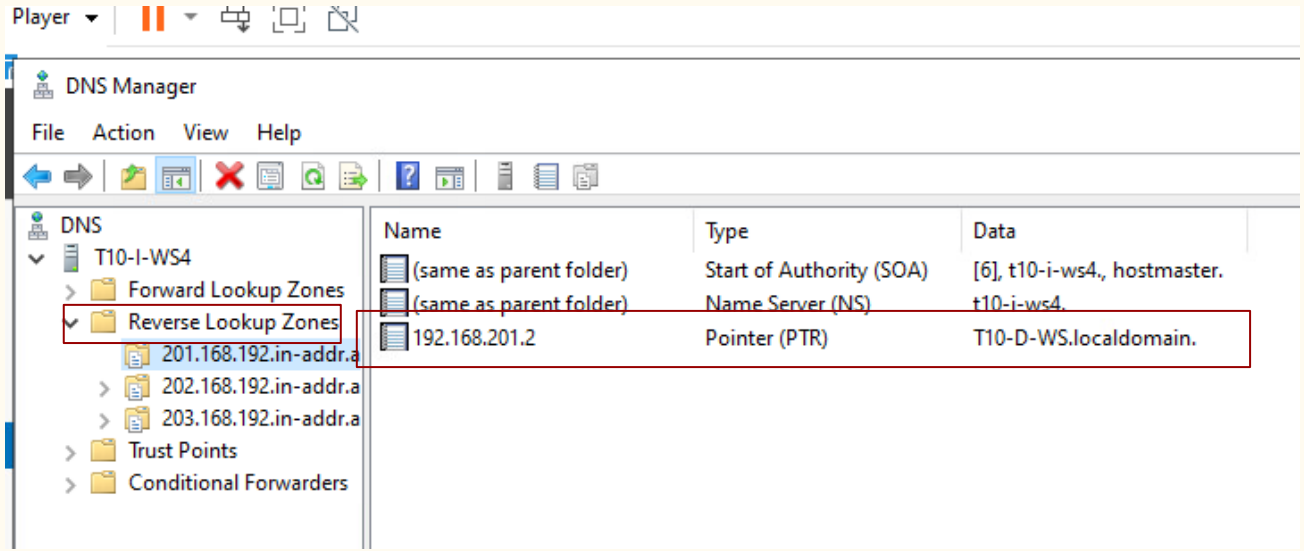
Check proper configurations.

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

>
```

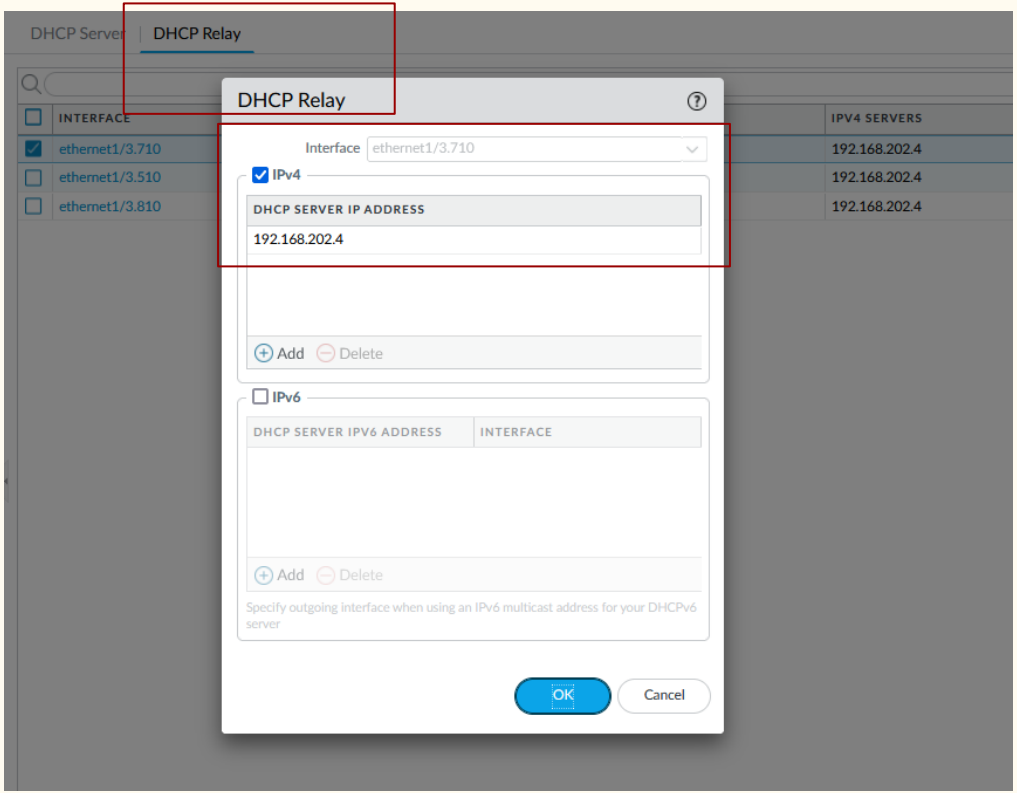
Configurations to allow DHCP broadcast through firewalls.

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

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

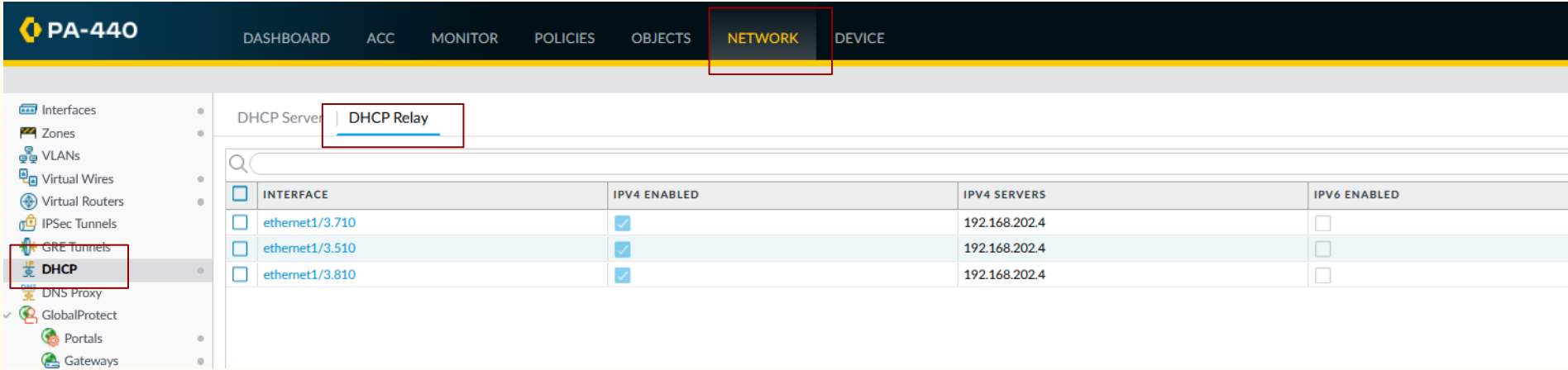
Configurations to allow DHCP broadcast through firewalls.

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.



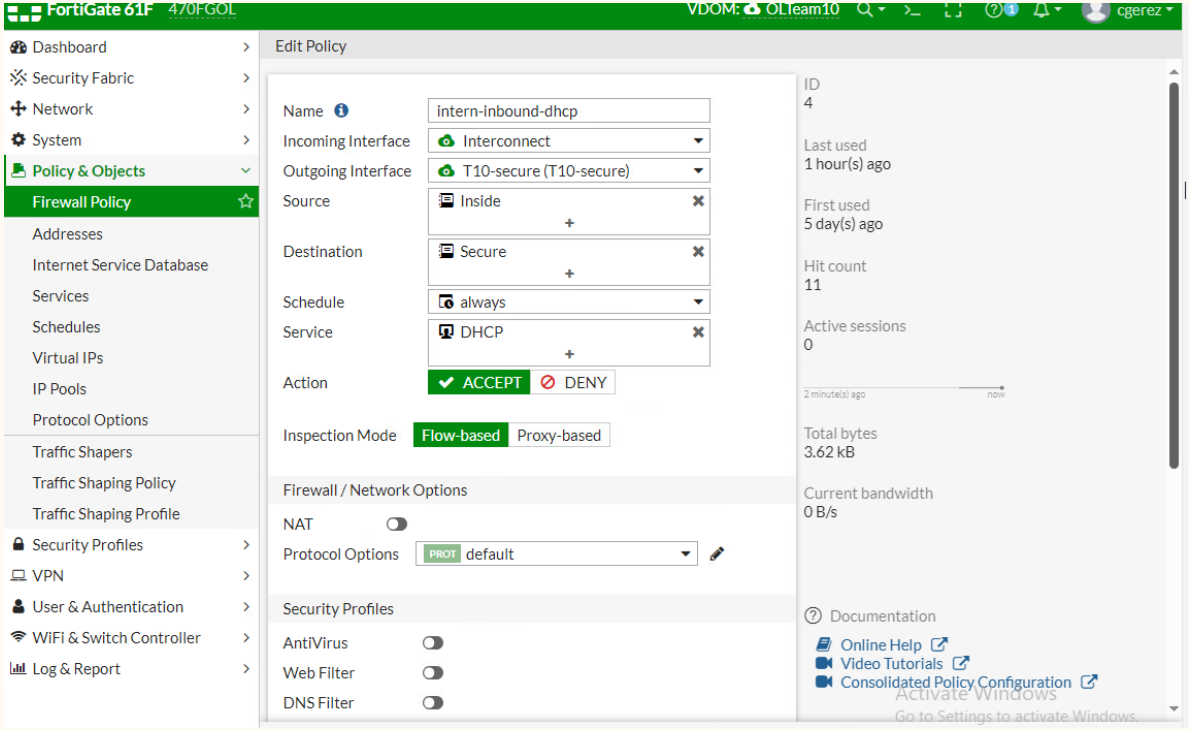
Configurations to allow DHCP broadcast through firewalls.

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



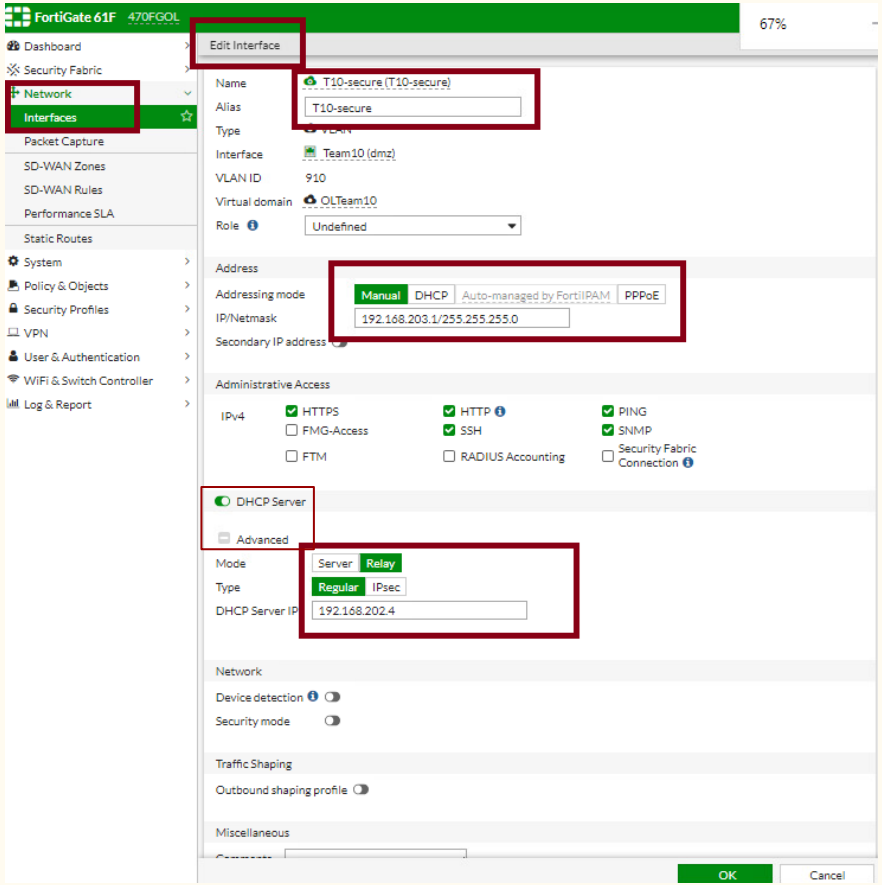
Configurations to allow DHCP broadcast through firewalls.

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