Lab Guide

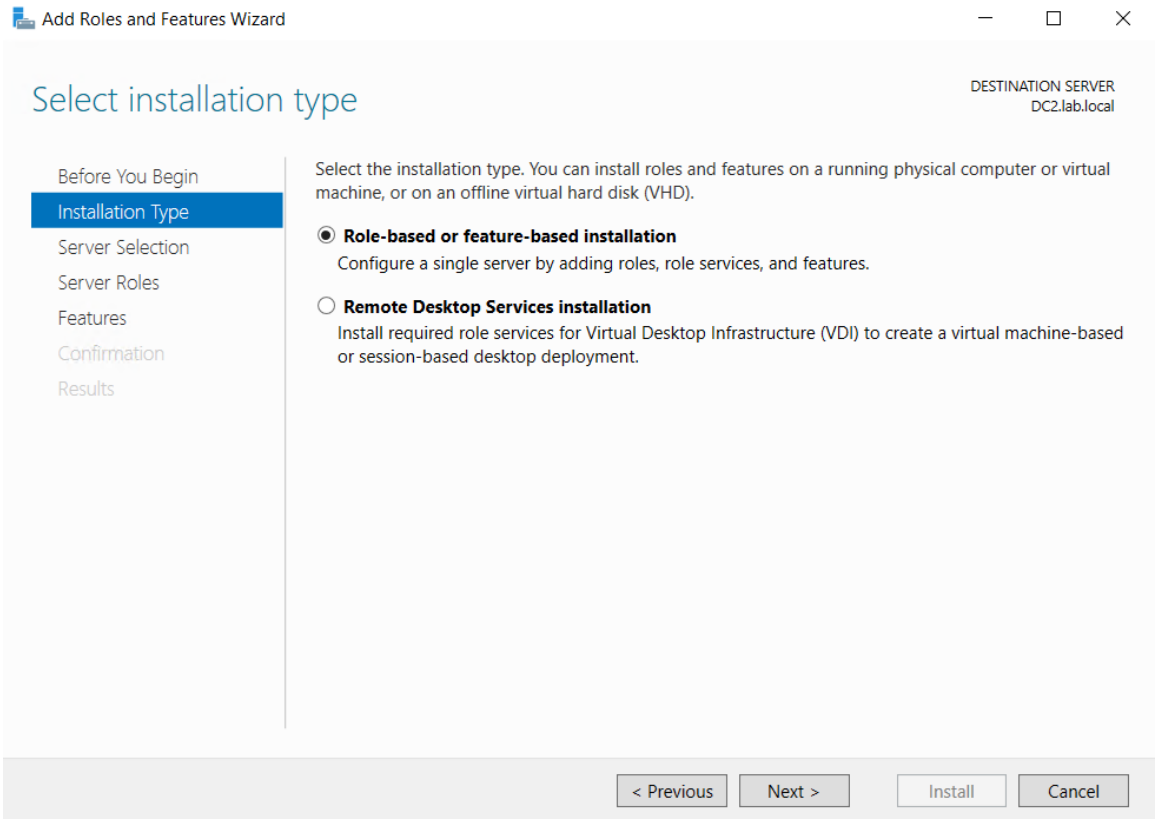
Implementing and maintaining DNS

Install DNS role

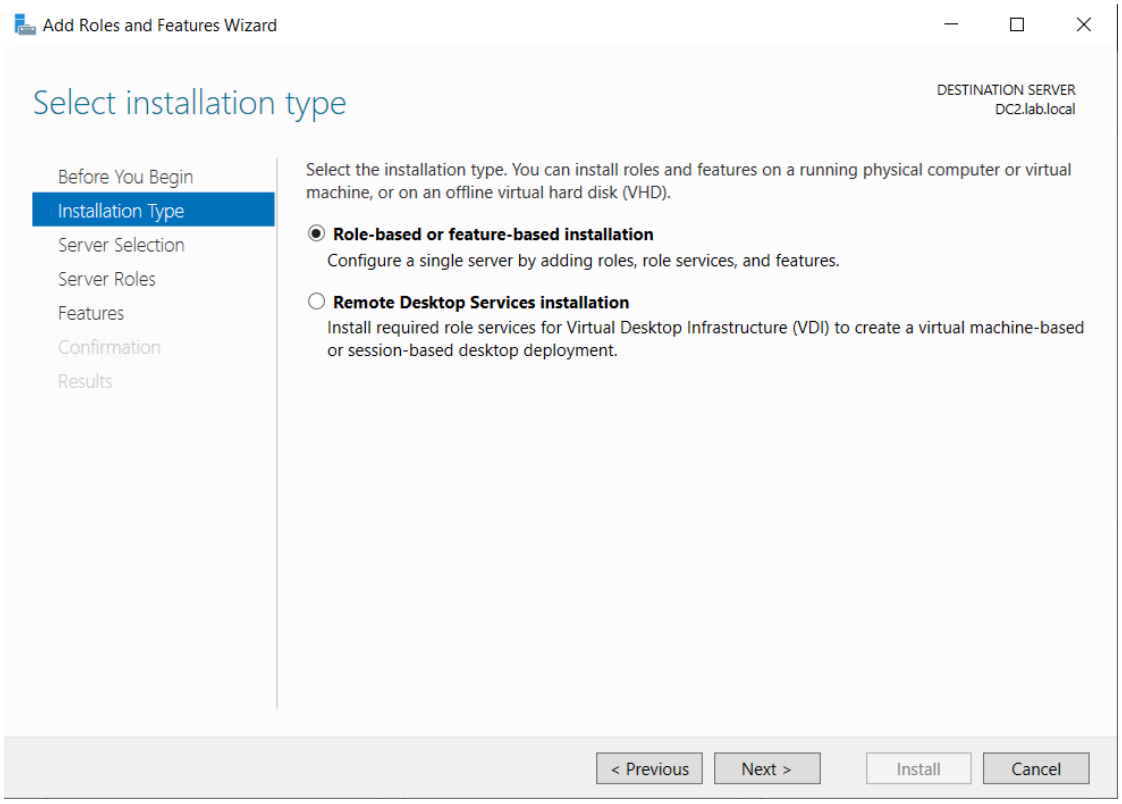
We have a running DNS service on DC1, which got installed when we installed the first domain controller in the domain “lab.local”

We will install another DNS server on DC2, and use it to get hands on experience in configuring and maintaining DNS service in Windows server environment.

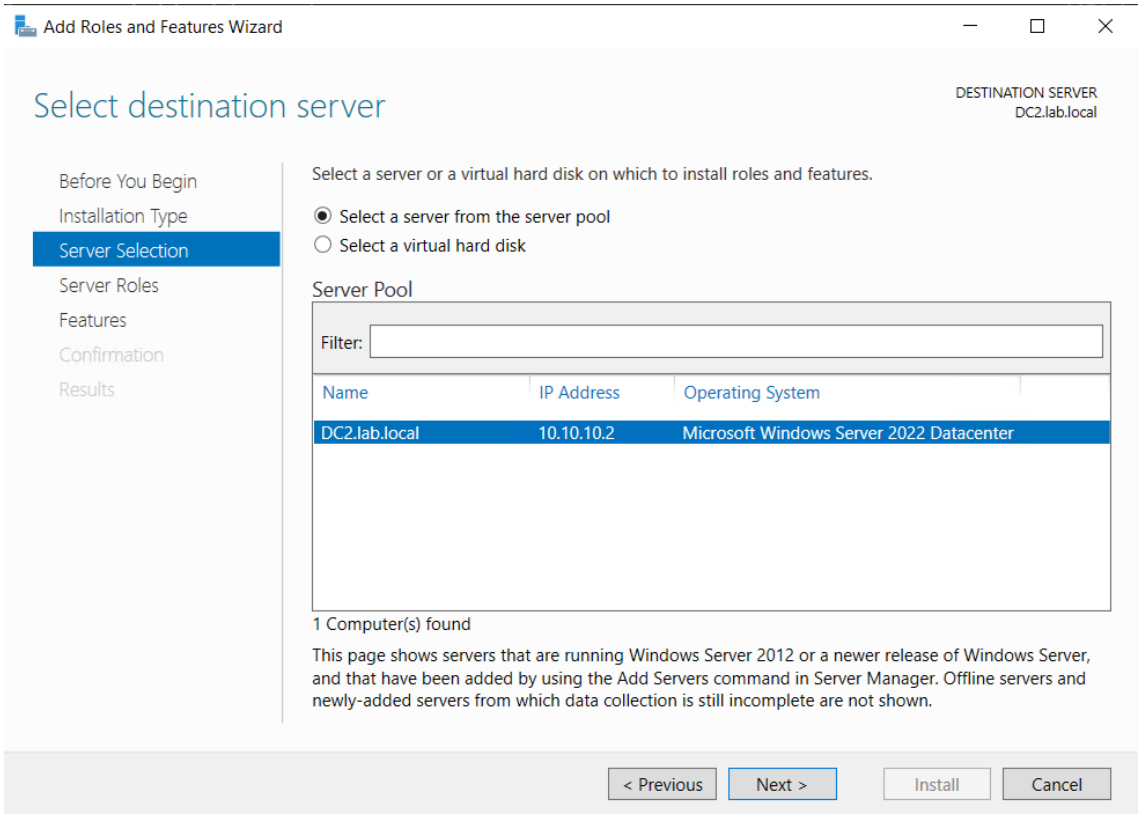
1- Open the Server Manager on DC2 and click on “Add Roles and Features”, then click “Next”.



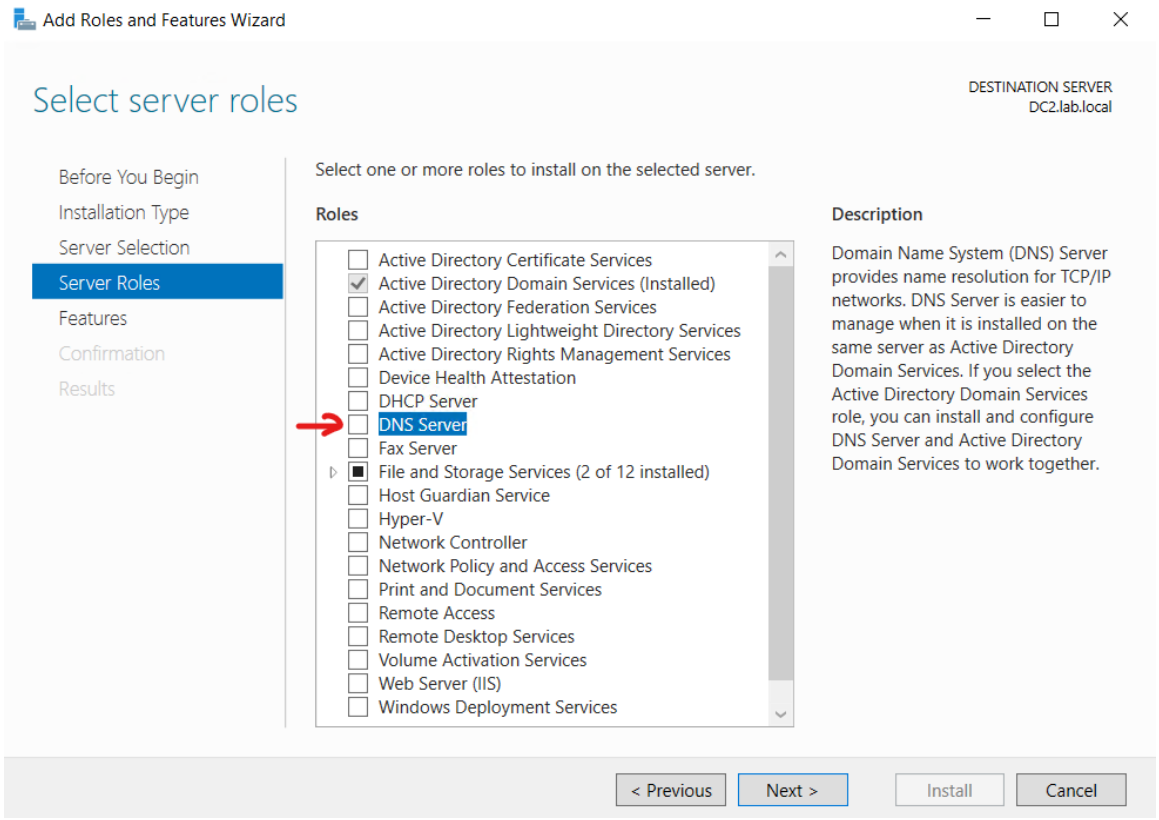
2- Keep the selection on “Role-based or Feature-based installation, and click “Next”



3- Make sure DC2 is selected and click “Next”.



4- Check on DNS, and click “Next”, then a message will popup asking to add the required features, click “Add Feature”, then click “Next”.

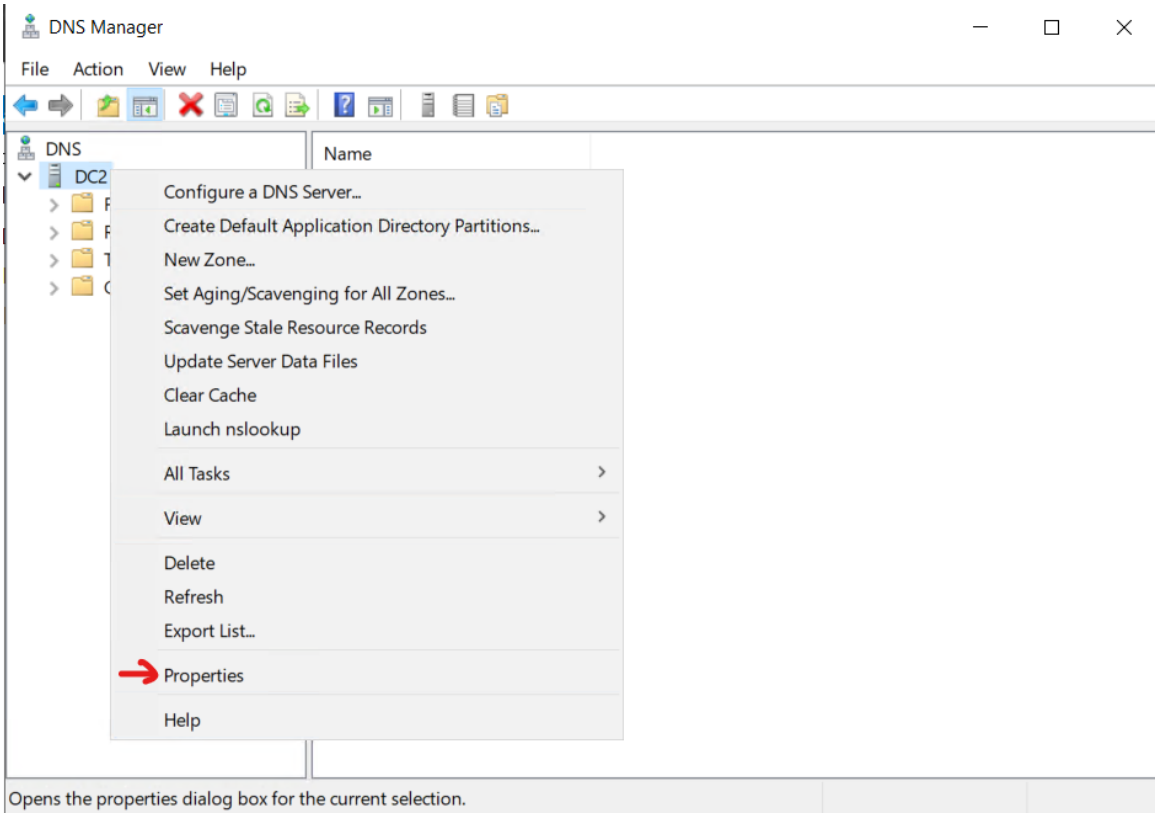


5- Click “Next” twice, and finally “Install”.

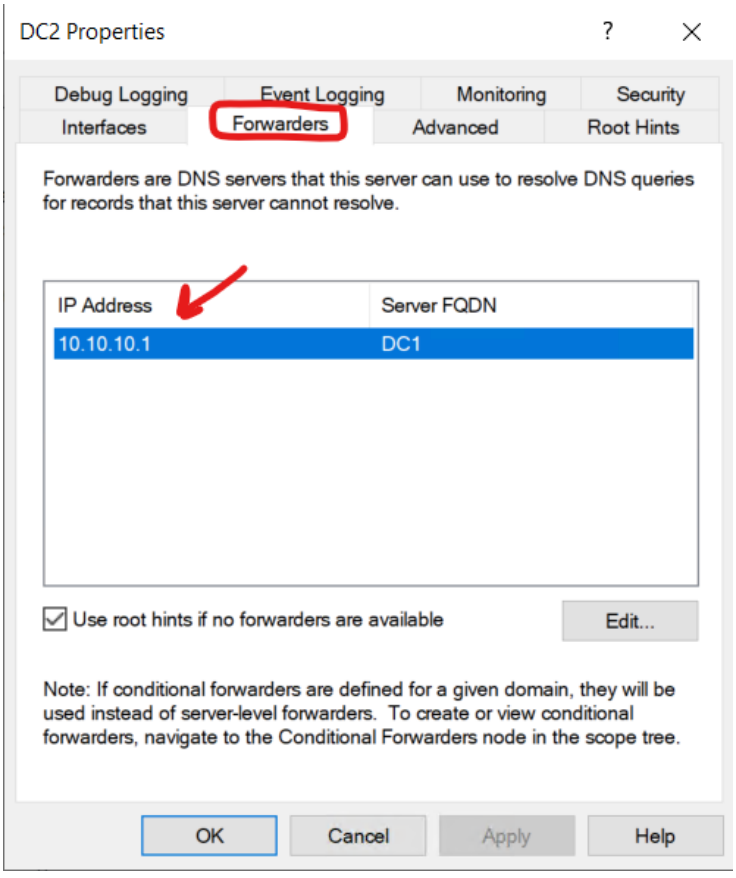
Now DNS role will be installed, the next step is to configure the server in order to make it able to serve client DNS queries.

DNS can respond to click queries by either checking its own “DNS Zone”, or be getting help from other DNS servers.

6- At first, you can configure the server as a forwarder which gets clients requests and forward them to anther server you specify.
To do that, go to “Server Manager”, click on “Tools” then select “DNS” from the menu
Then will open the DNS console, right-click on the server’s name and choose “Properties”



7- In the "Properties" page click on "Forwarders" tap, then add DC1 as shown in the picture



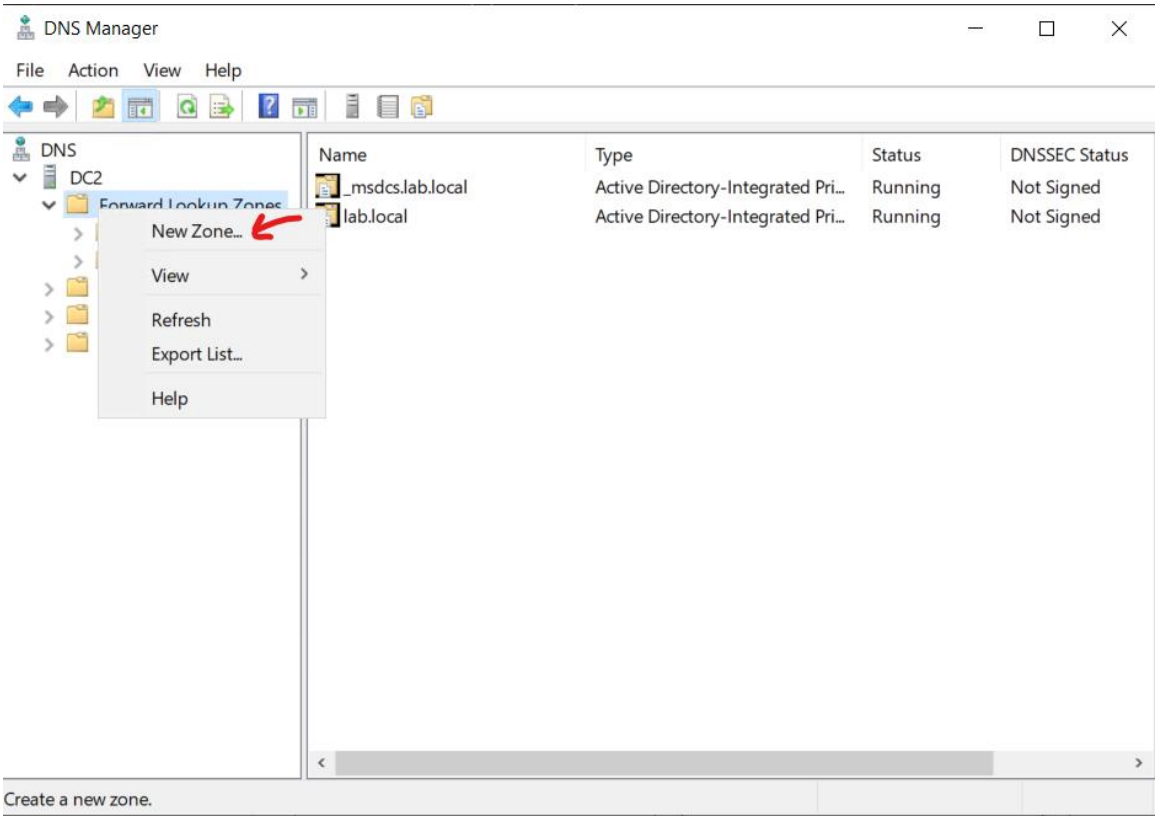
Now DC2 will respond the client queries by forwarding the query to DC1, getting the response, and send back the response to the client.

Primary and Secondary zones

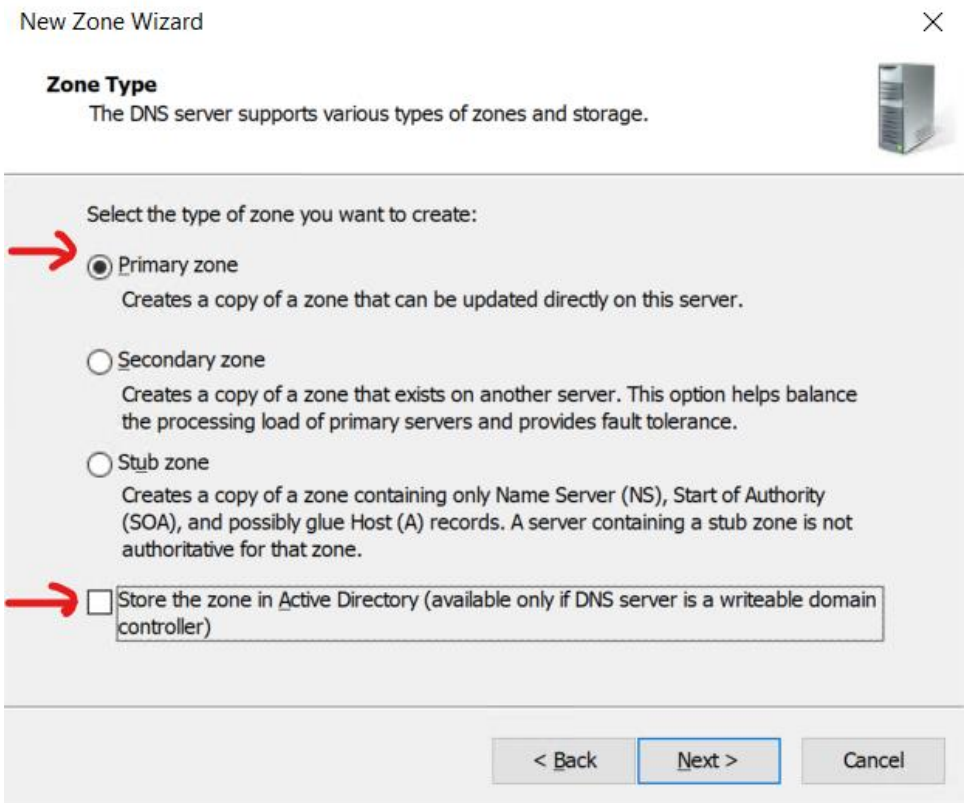
Let's go further with the next step which is to add a new zone to DC2 to make it able to respond to client queries by itself.

At first, we will create a Primary zone and configure zone transfer with a secondary zone on another DNS server.

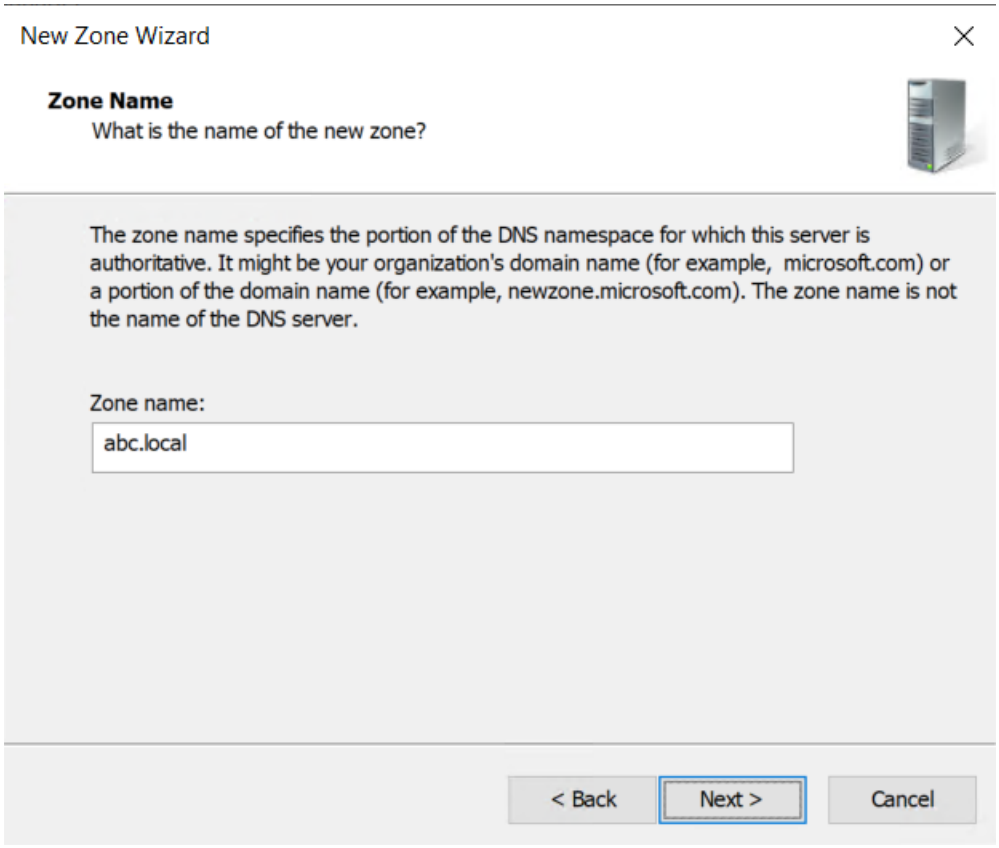
8- In DNS console on DC2, make sure forward lookup zone to selected, then right-click on it, and choose "New Zone"



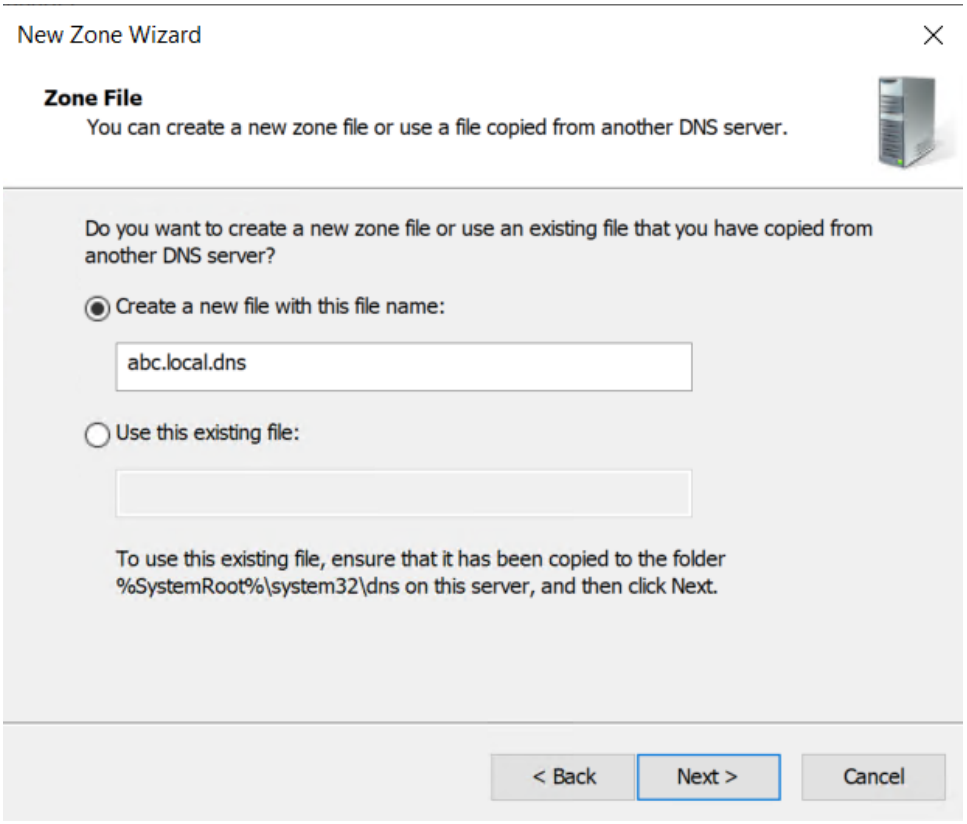
9- In the "New zone wizard" click "Next", then leave the default selection on "Primary zone", and uncheck the option down the window, which says "Store the zone in Active Directory, (this option is available only of DC2 is already and domain controller. Then click "Next"



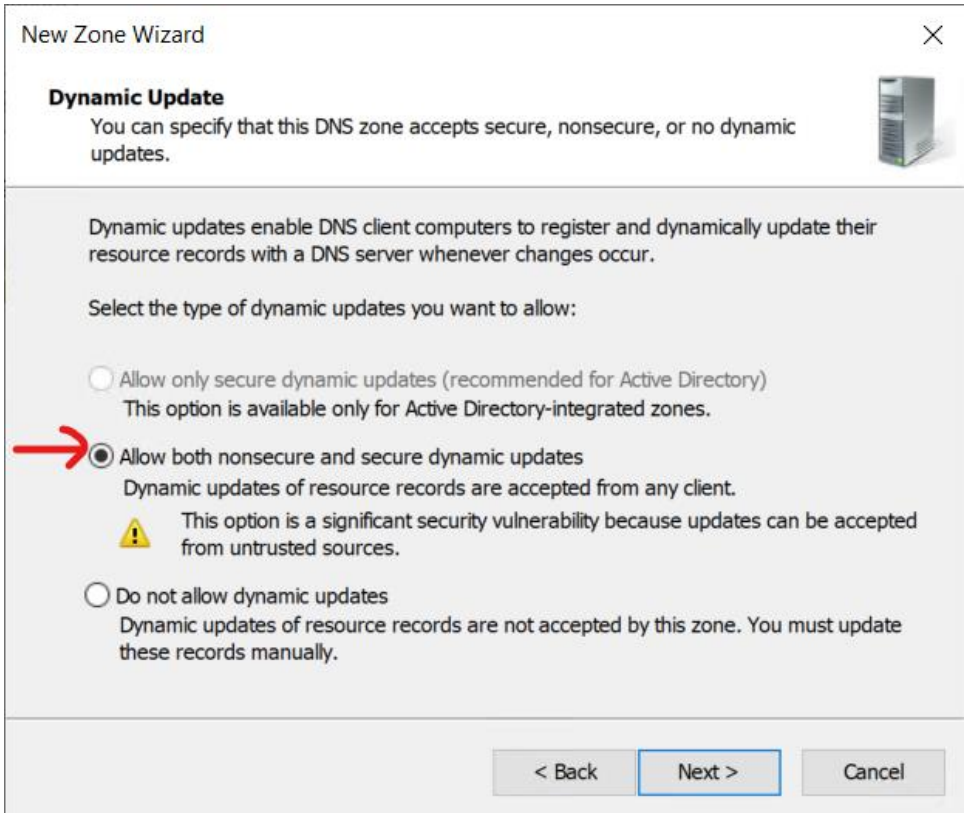
10- Enter the new zone name “abc.local” and click next.



11- In the zone file name accept the default, and click “Next”



12- In the “Dynamic Update” window change the selection allow both secure and nonsecure dynamic updates, and click "Next"

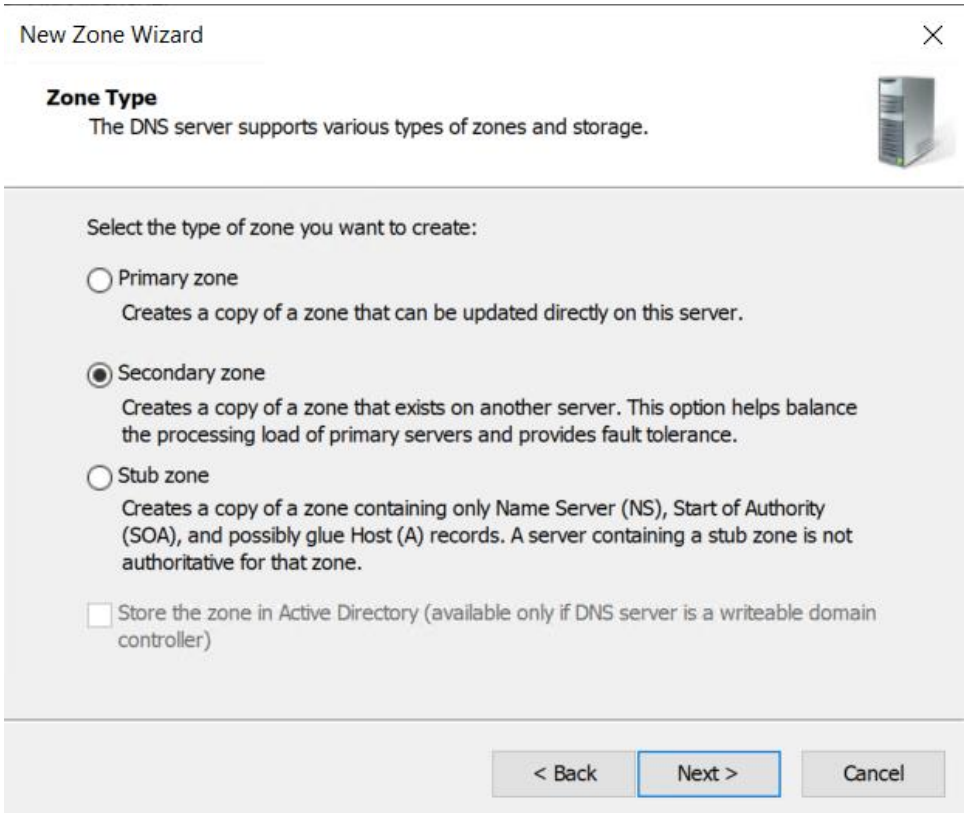


13- Click “Finish” to create the zone.

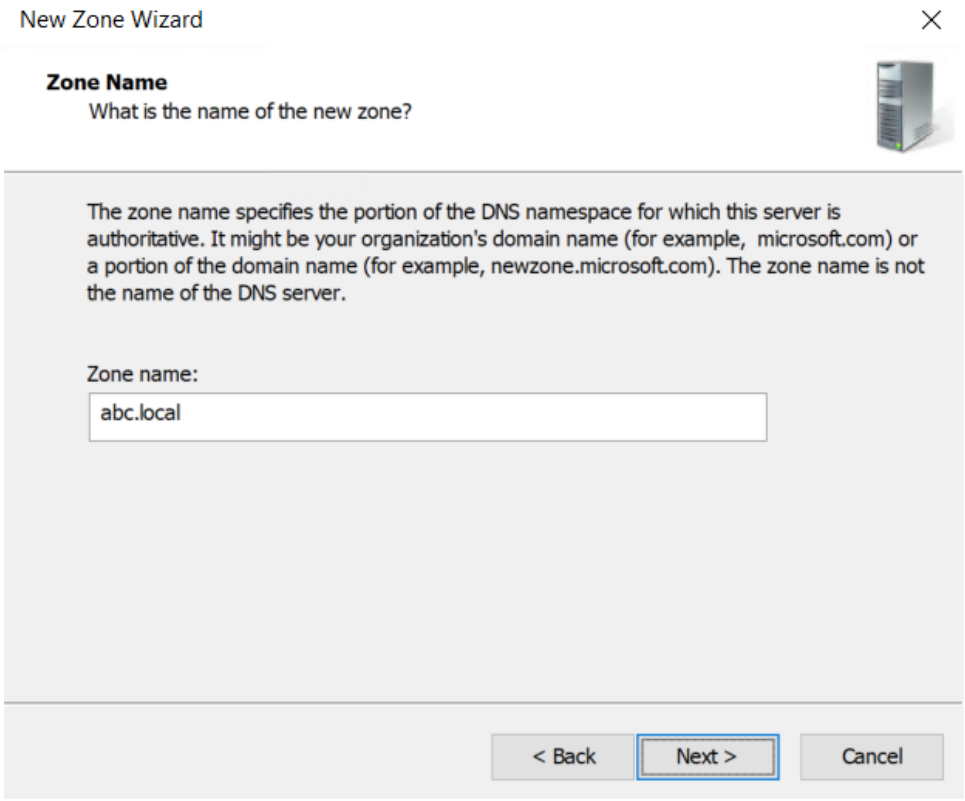
Now the zone is created as a primary zone, and we need to create a secondary zone on another server, which will be read-only zone, and will transfer it is records from the primary (the master)

We will use DC1 for this step

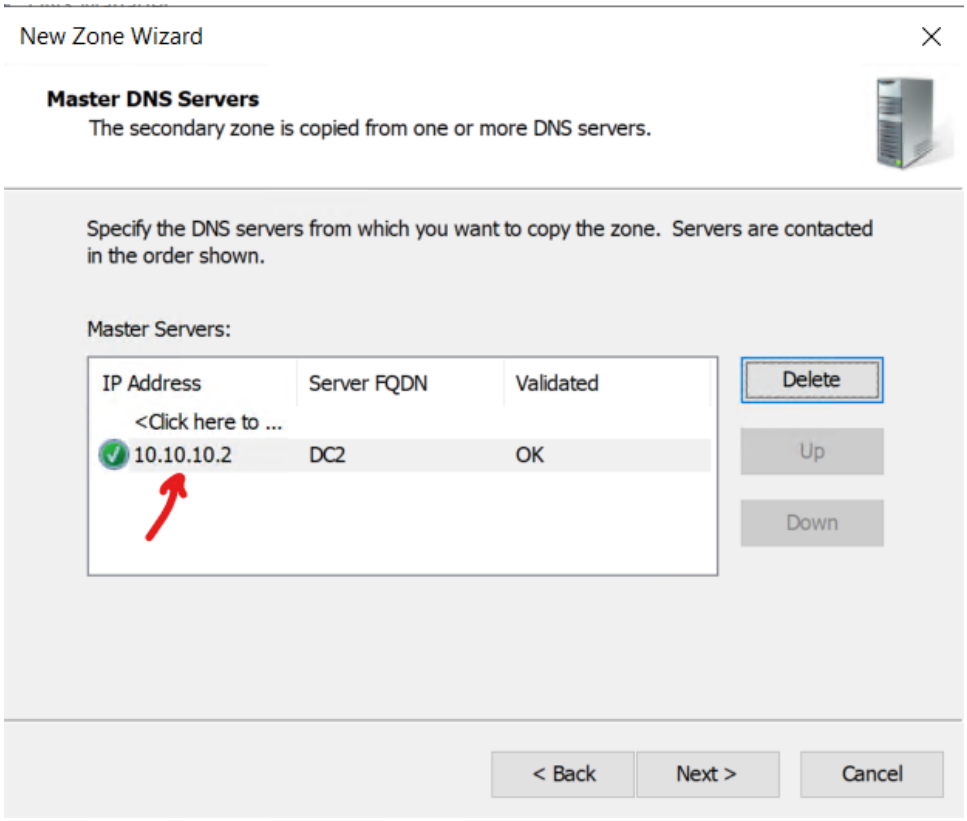
14- , Go to DC1, Open the DNS console then r-click on the server’s name and choose “New Zone”, and select secondary, then click “Next”



15- Enter the zone name “abc.local”, then click “Next”



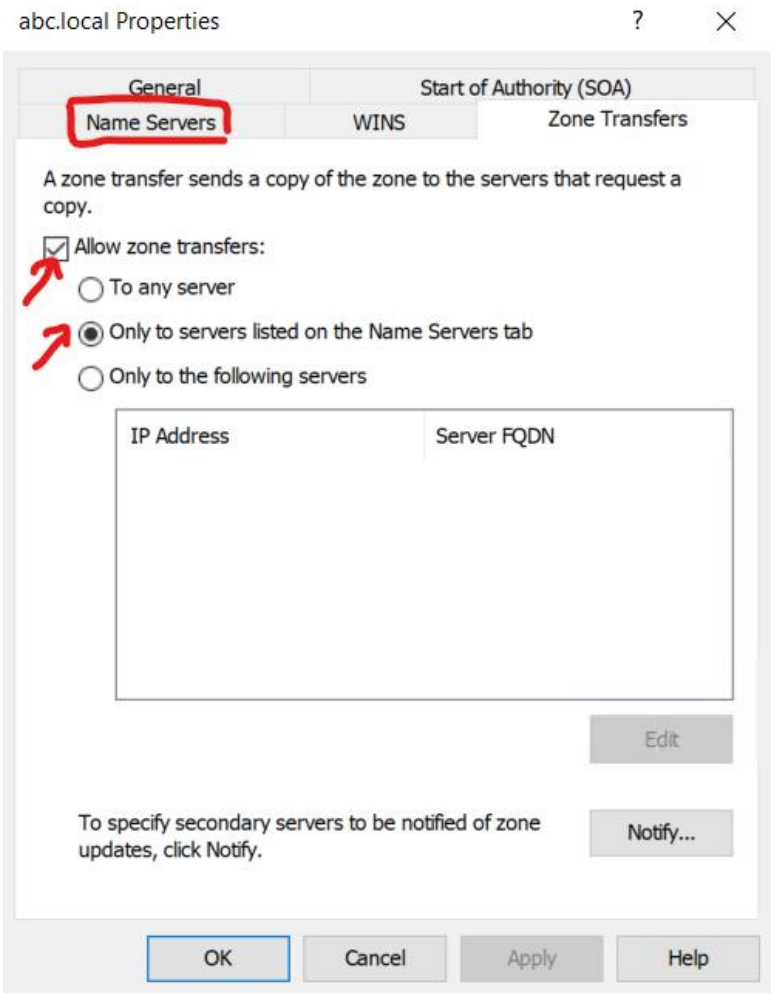
16- Enter the IP address or the name of the DNS server which holds the primary zone, in our case it is DC2.



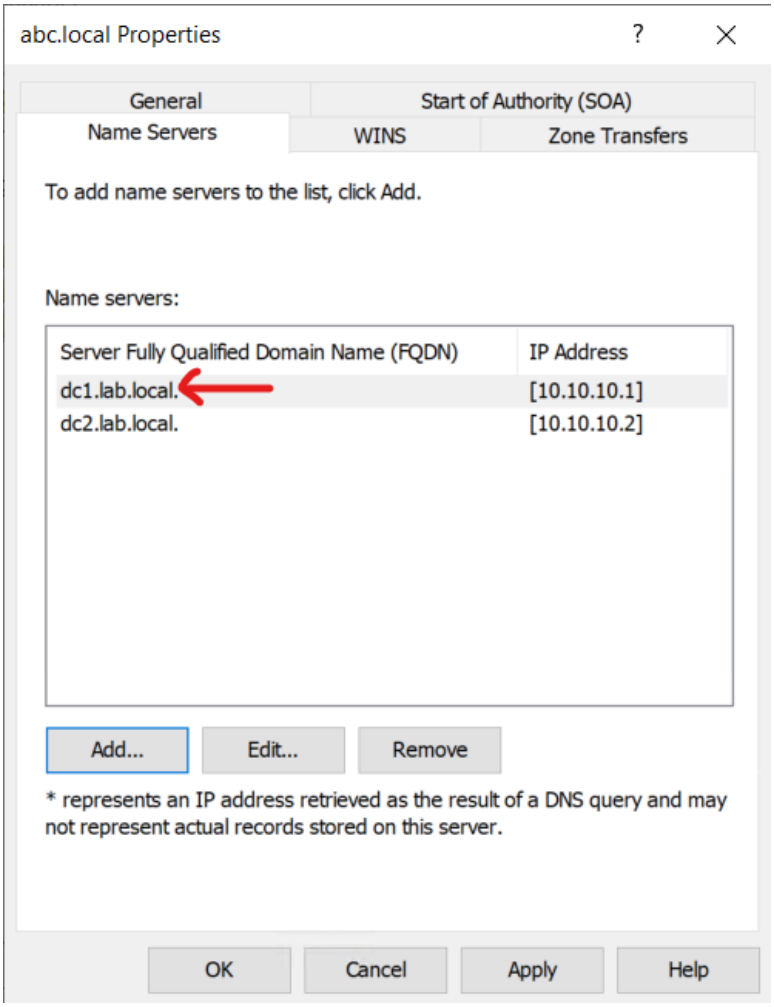
17- Finally click finish the create the zone.

Now the zone is created but we need to allow zone transfer from DC2 (the master) to DC1, before allowing zone transfer from the master, the secondary zone will not work.

18- Go to DC2, r-click on “abc.local” zone and choose properties.
19- Click on “zone transfer” tap, it says that transfer is allowed to server that are listed on “Name Servers” tap



20- The point is “Name Servers” tap has only DC2, and we need to add DC1 (which has the secondary zone) in it.



21- Wait a minute for the transfer to happen, and you can refresh the zone on DC1 to see that transfer has been successful.

22- Create a new “Host (a)” record on the primary zone, and check if the zone transfer has been successful in the secondary zone.

23- Try to create a new record on the secondary zone, you won’t find the option to do so. As this copy of the zone is read only.

Active Directory Integrated Zone

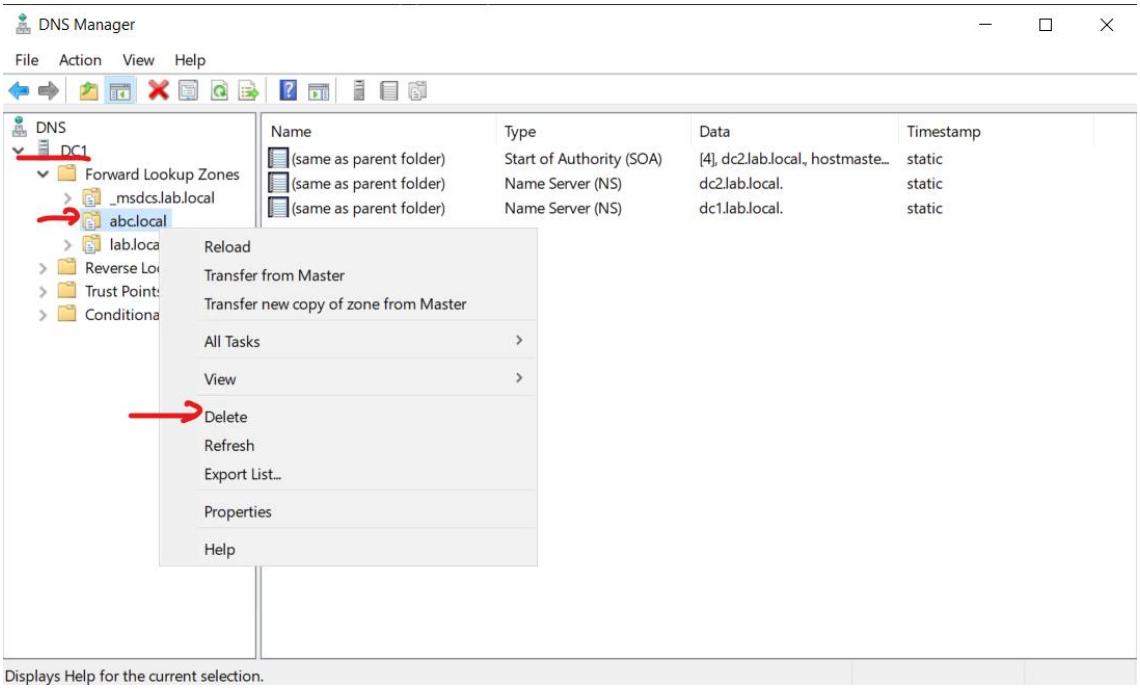
Benefits of DNS integrated Active Directory

- Multimaster update and enhanced security based on the capabilities of Active Directory.
- Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an Active Directory domain.
- Directory replication is faster and more efficient and secure than standard DNS replication.
- Multiple masters are created for DNS replication. Therefore, any domain controller in the domain running the DNS Server service can write updates to the Active Directory-integrated DNS zones.
- Secure dynamic updates are supported.
- A forest-wide application directory partition is available in this scenario, called ForestDnsZones.
- Domain-wide application directory partitions for each domain in the forest, named DomainDnsZones.

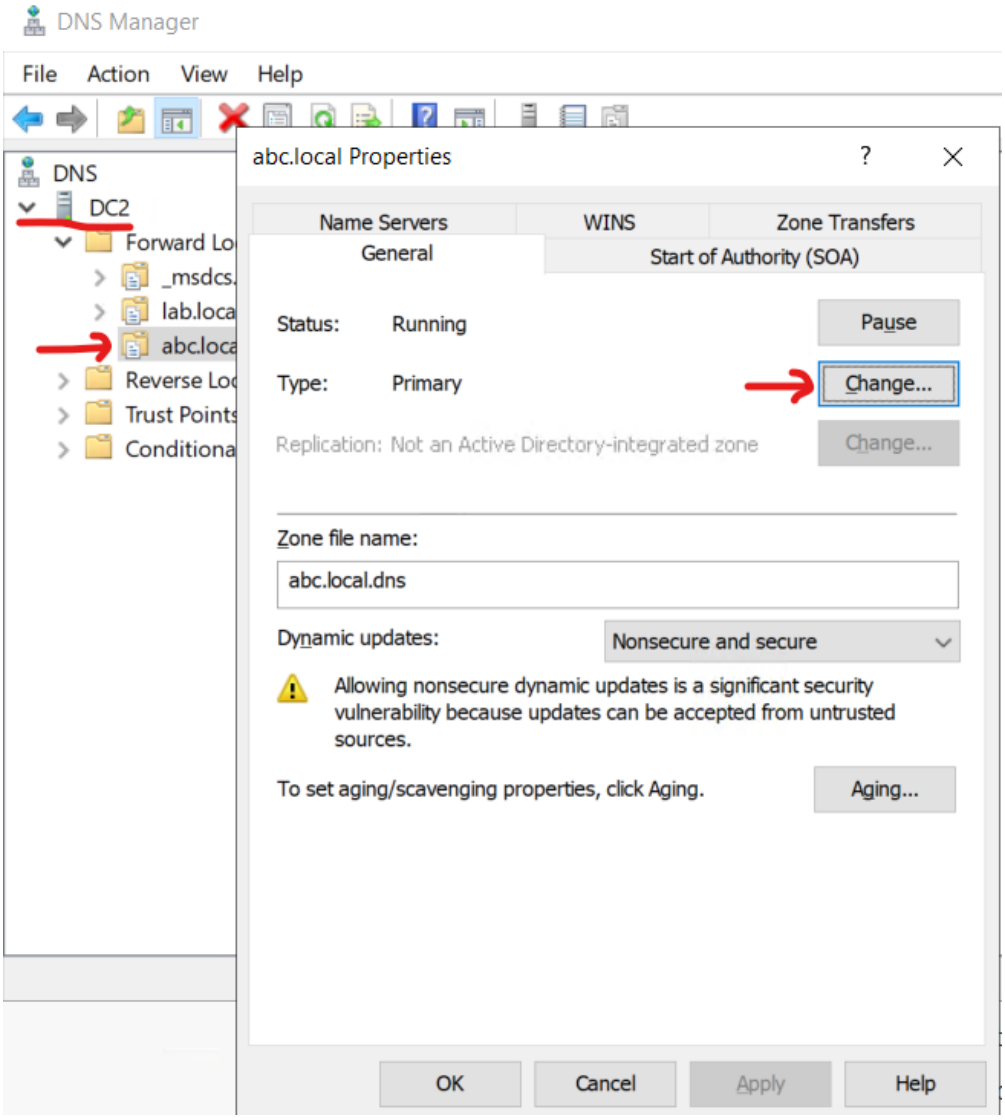
To get the benefits of DNS integrated Active Directory, the steps are very simple, we will delete the secondary zone “abc.local” from DC1. Then convert the primary zone on DC2 to an Active Directory integrated zone.

Please notice that both DC1 and DC2 are domain controllers.

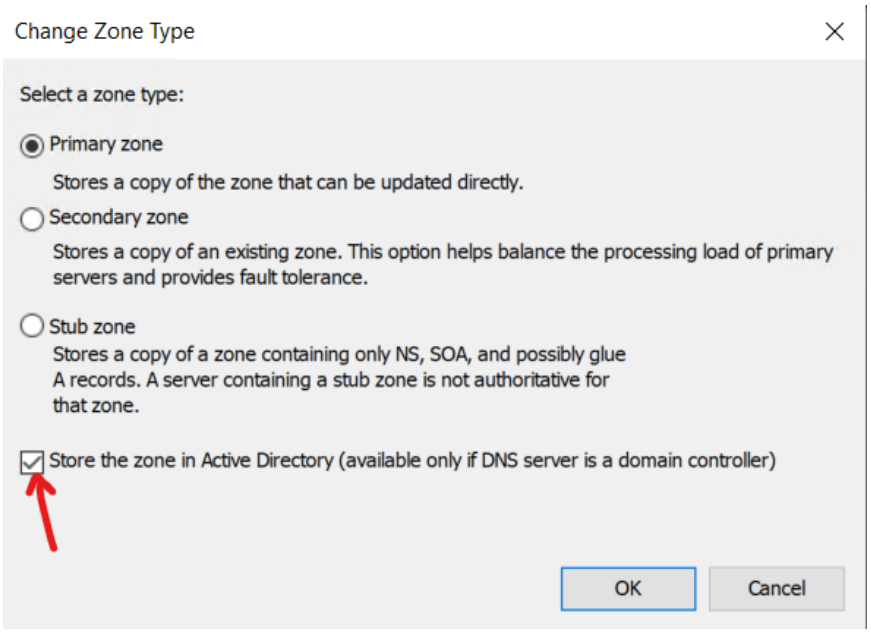
24- Delete the secondary zone from DC1



25- Open DNS on DC1 and r-click on the zone and choose properties, then click on "Change"



26- Check on the option to store the zone in Active Directory, then click "OK".



27- In the confirmation message, click “Yes”
28- Click “Ok” to close the properties window.
29- Now, we just have to wait just minutes for the replication to take place, and the zone will appear on DC1 with the latest updates with no further configuration.