SCHOOL OF COMPUTING

DIPLOMA IN INFOCOMM SECURITY MANAGEMENT

ST2612 SECURING MICROSOFT WINDOWS

ASSIGNMENT

Class: DISM/FT/2A/23

Name: Md Amirul Adeeb Bin Rizal (2107095)

Securing Active Directory Operations

Table of Contents

1. Summary

As one of the few primary concerns in the IT sector, load balancing, security, and high availability are the three main areas of focus for the Dynamic Host Configuration Protocol (DHCP). Without load balancing, security, and availability, it is difficult for an organization to protect itself from an attacker's attack while still offering uninterrupted service to its customers. The use of load balancing will improve traffic flow and avoid network congestion. Client productivity won't be impacted by a server that can run continuously without any downtime thanks to high availability configuration. The report will include setup requirements as well as a few security features that boost each of the three main services productivity and security. It will offer suggestions for features that could be implemented differently to produce different results.

2. Introduction

2.1 Main Objective

Two domain controllers will be used in the configuration, and the three primary services—Active Directory Domain Services (ADDS), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP)—will be covered in terms of high availability, load balancing, and security of a domain network. Even if one or both Domain Controllers are offline, the setup is set up to continue operating without interruption.

2.2 Prerequisite of system

The prerequisites for setting up the domain network are the main topic of this section.
It would be necessary to have:

- The next would be required: 2 Windows Server 2016 Virtual Machine
- 1 Windows 10 Virtual Machine
- VMware Workstation Pro (Version 16 or later)

3. Setting up the Domain Networks

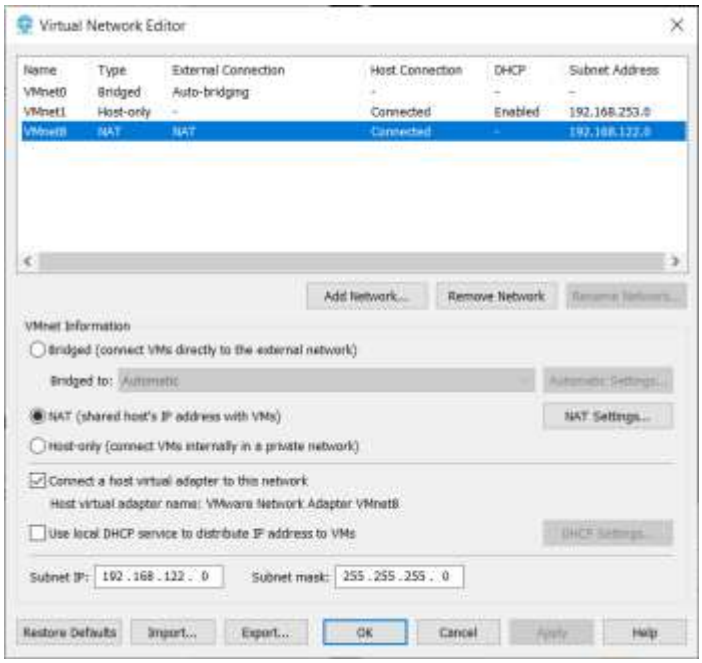
The steps required to set up a domain network are covered in this section. In this case, there will be two domain controllers (DC), both of which will be within the same domain. The operating system for both domain controllers will be Windows Server 2016.

3.1 Setup for 1st domain controller

The steps below will be on the setup of the first domain controller. Make sure you turn DHCP on first when you first use the VM then you can turn it off.

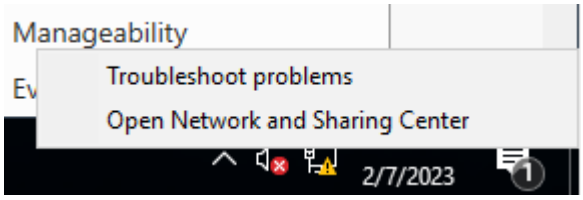
3.1.1 Set the Static IP Address

1. Start VMware Workstation. Go to edit, Virtual Network Editor.



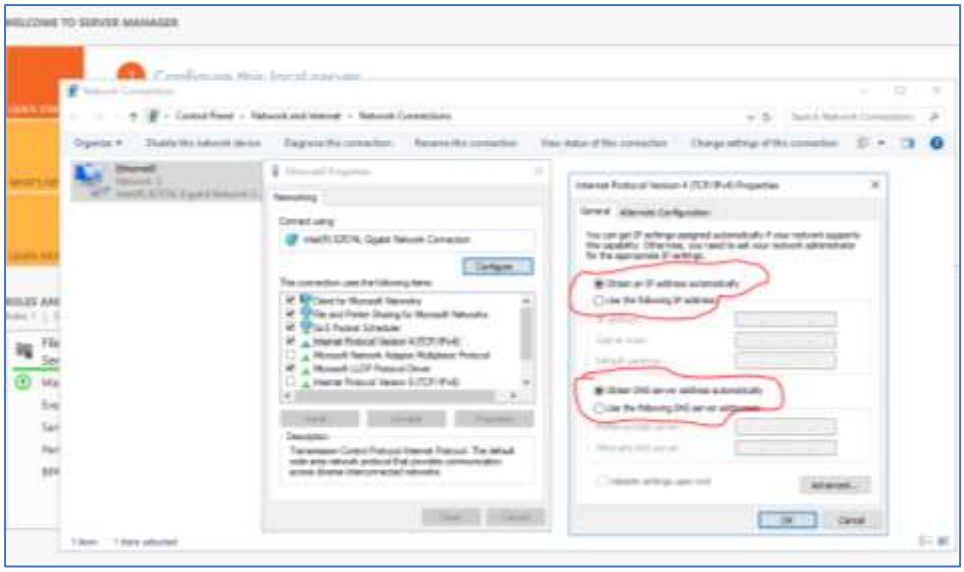
2. Select VMnet8. Ensure "Use local DHCP service to distribute IP address to VMs" is not tick and take note of your subnet IP range.

3. Power on your image and login with your credentials.



4. Open "Network and Sharing Center" by right click on the internet icon on the bottom right of the taskbar.

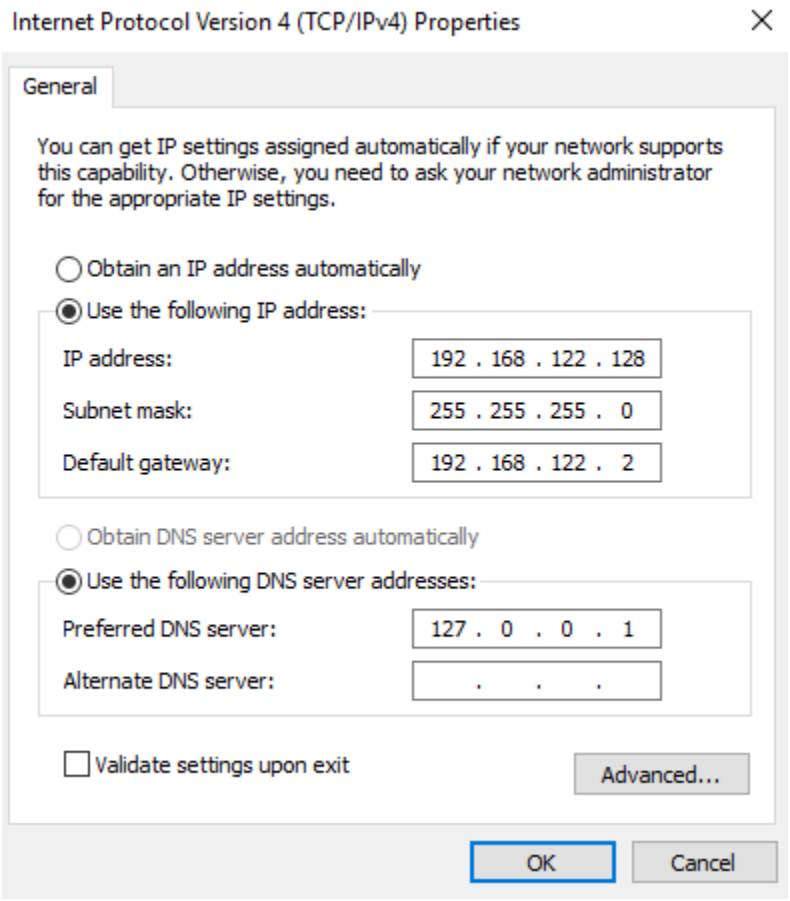
5. Press the 'Change Adapter Settings'



6. Right click on the ethernet adapter. Select Properties

7. Double click on ‘Internet Protocol Version 4 (TCP/IPv4)

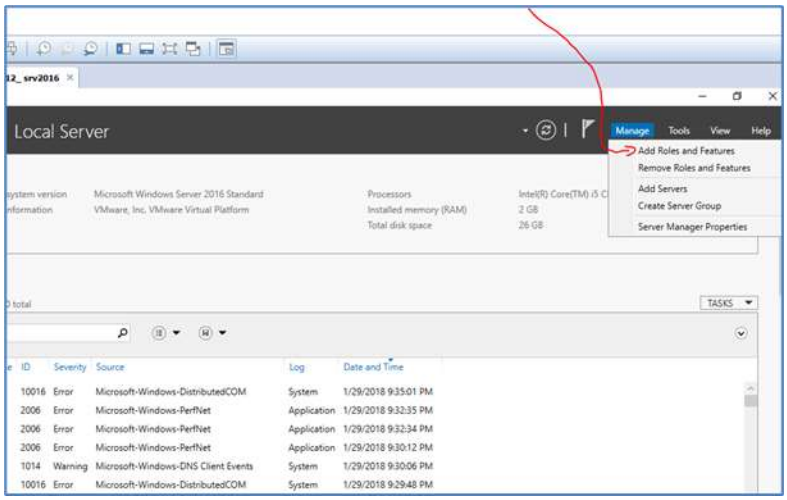
8. Modify IP address, Subnet mask and Default Gateway Server to a valid static value (IP address first 3 octets should be the same as the IP shown in step 8)



3.1.2. Install Active Directory Domain Services (ADDS)

We will now install Active Directory Domain Services to make our Windows Server 2016 into a Domain Controller.

1. To add ADDS role: At server manager, on the top right click on Manage> Add roles and features

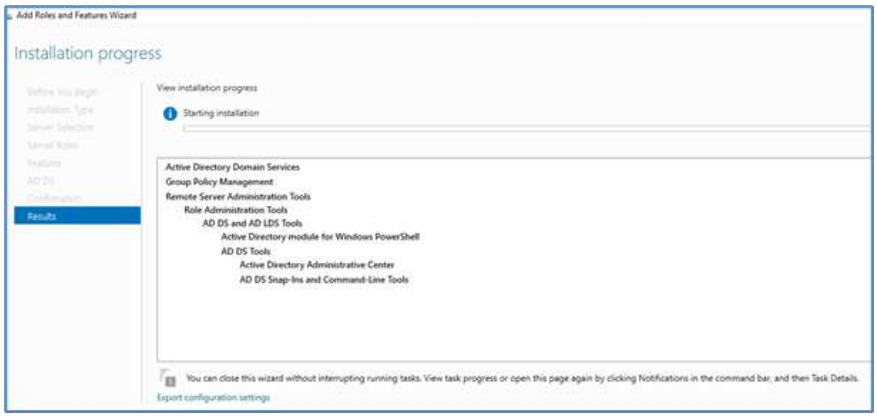


2. Press next. Choose ‘Role-Based or feature-based installation`. Press next.

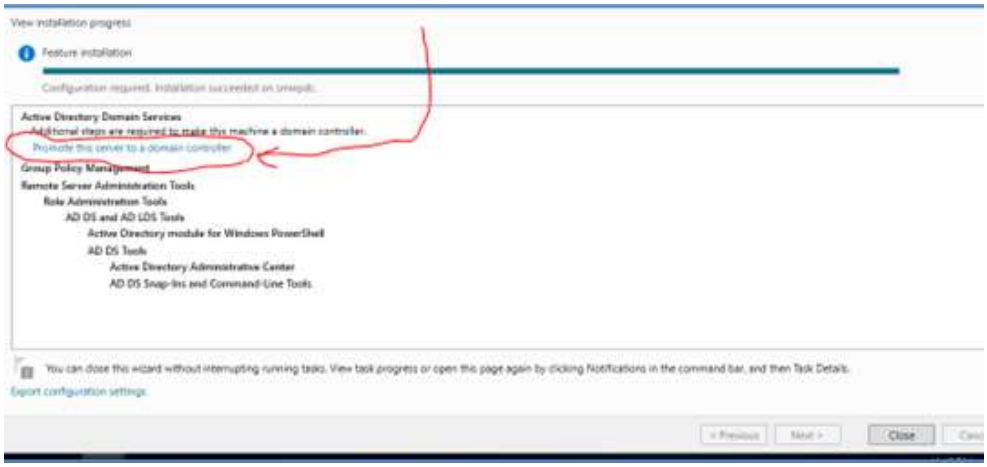
3. Under Server Selection, select 'Select a server from server pool and select your server. Press Next.

4. Under server roles, choose "Active Directory Domain Services. A pop up will appear and choose 'Add features' press next.

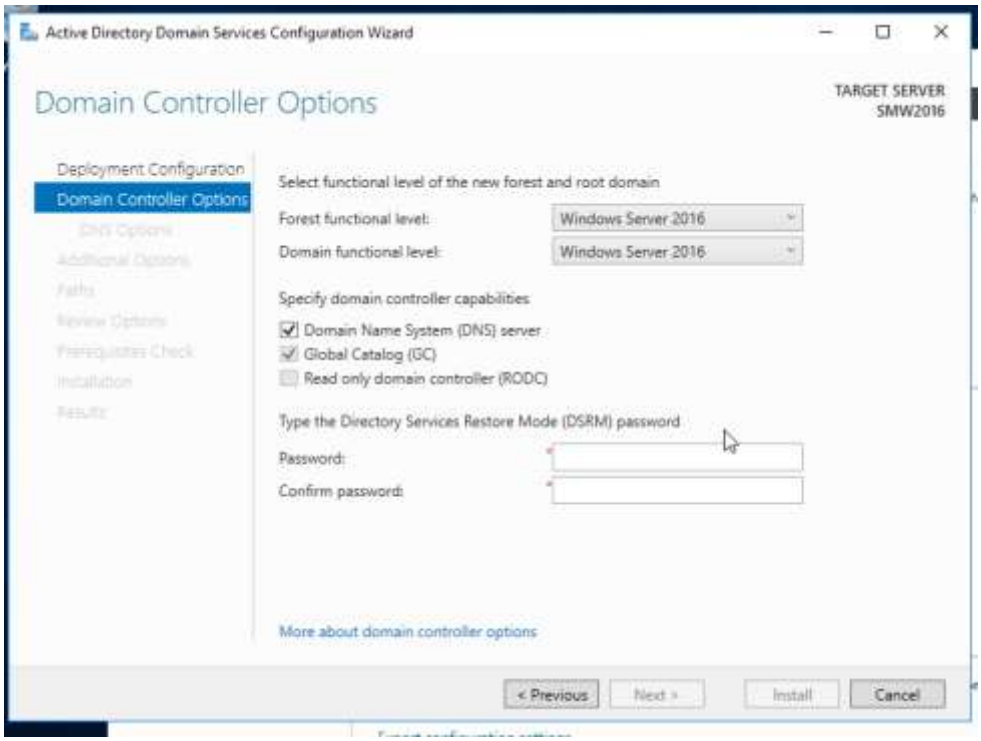
5. Accept all default options given and click next till the installation page and click install. (Image below shows the installation of ADDS)



6. After installation is done, don’t forget to promote the server to a domain controller by pressing the flag on the top right of server manager.

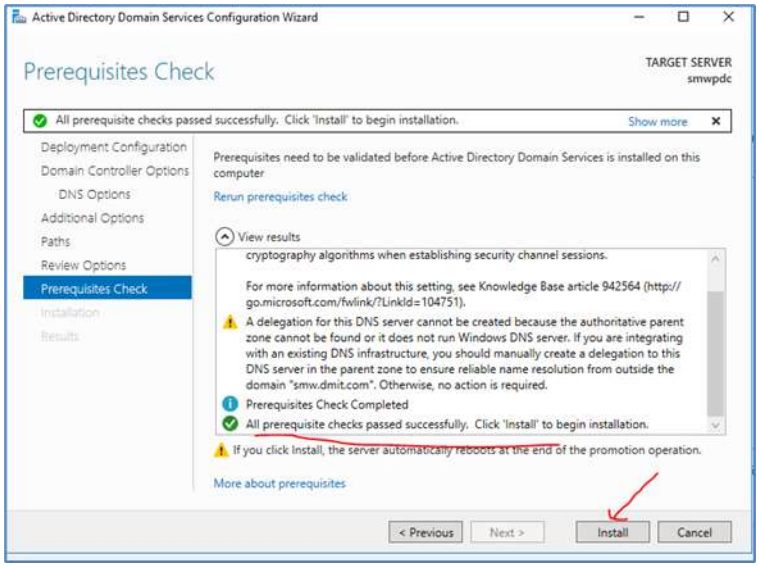


7. A configuration wizard to promote server to domain controller will appear.



8. Press next forest and domain functional level as set at Windows Server 2016 Ensure Domain Name System (DNS) server clicked. Provide a password. Press next.

9. Take the default options for DNS options and Additional Options and Path
10. Review your options. To proceed, Press next.



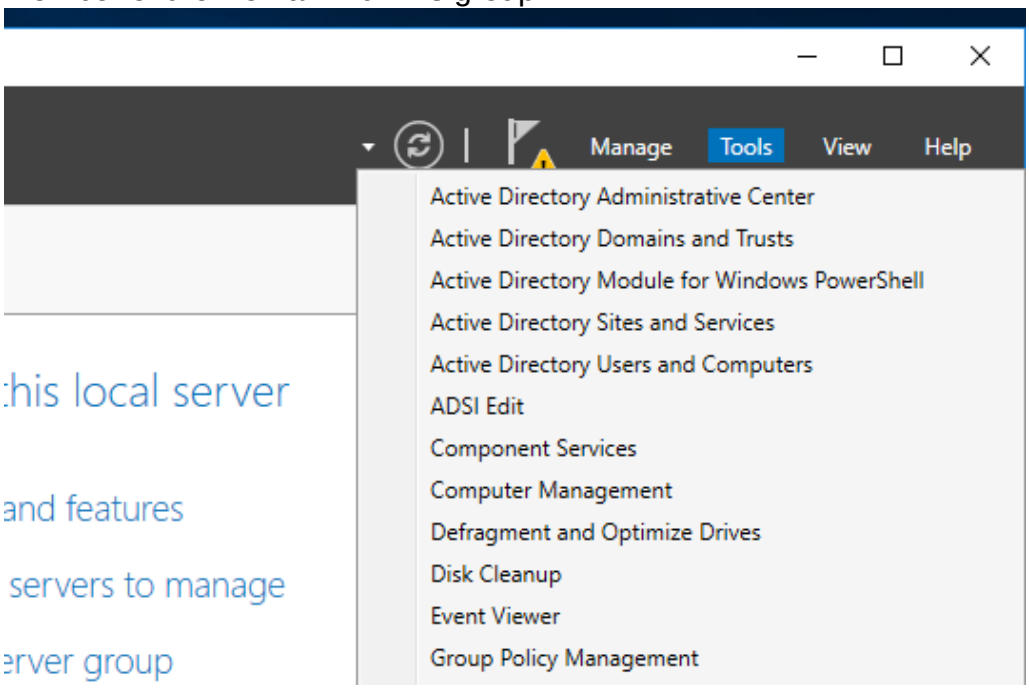
11. You may begin to install if the prerequisites check is successful.

12. After the installation is done, your server will automatically restart if it does not, manually restart your server

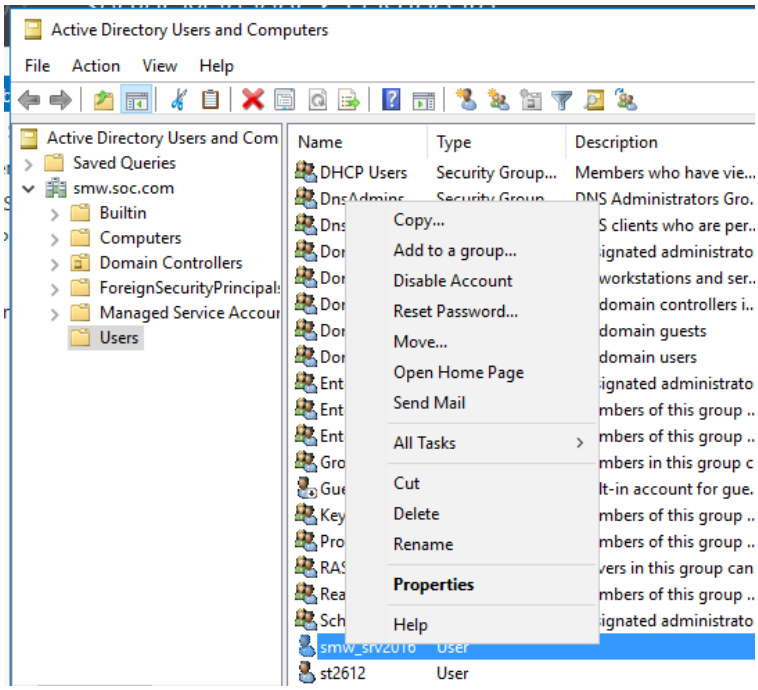
3.1.3. Install DHCP Service

To assign IP addresses to computers that will later connect to the domain after the server has been promoted to domain controller, DHCP service must be installed. The user account installing the service must be a member of the Domain Admins group to successfully install DHCP to the DC.

1. We can check Active Directory Users and Computers to see if the user is a member of the Domain Admins group.

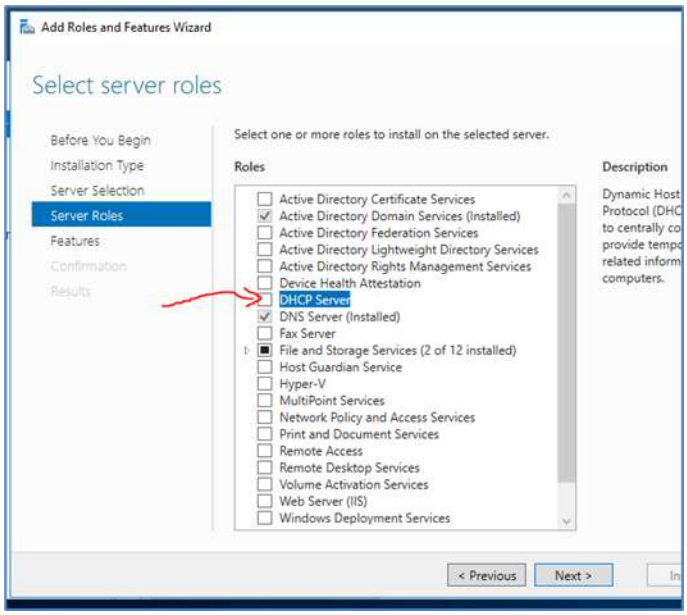


2. Expand your domain name. Under users, right click on the user account and click ‘Properties’.



3. Press Add, search for Domain Admins, click OK and click apply.

4. We have met the prerequisite to install DHCP service. Click on Manage > Add Roles and features.



5. Pick the default options until you are at Server roles page. Choose ‘DHCP Server’ and Add Features

6. Accept the default settings and install DHCP server.

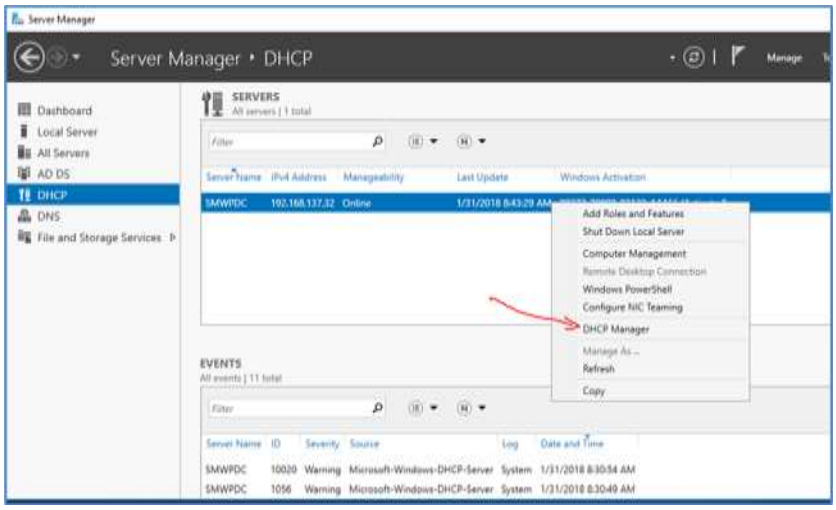
7. After installation, you are still required to complete the post-deployment configuration by clicking on the top right-hand side of server manager.

8. Accept all the default options and click commit

3.1.4. Configure DHCP Scope

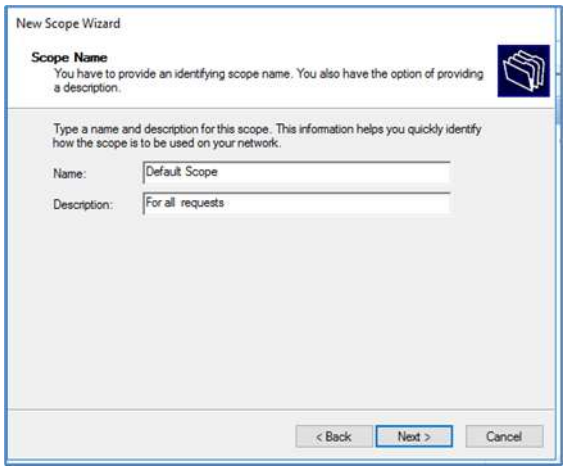
DHCP must be started in order to configure the scope, which determines the data that must be sent to every connected DHCP client.

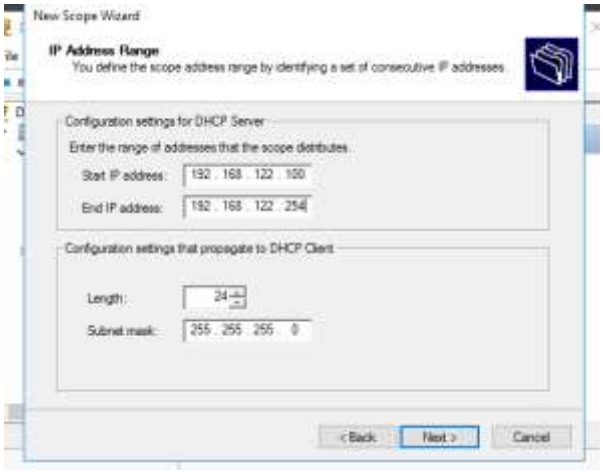
1. Access to DHCP Manager under Server Manager by right pressing the domain controller.

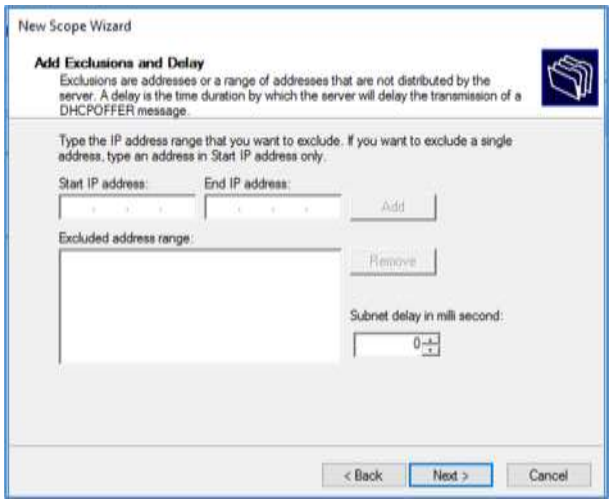


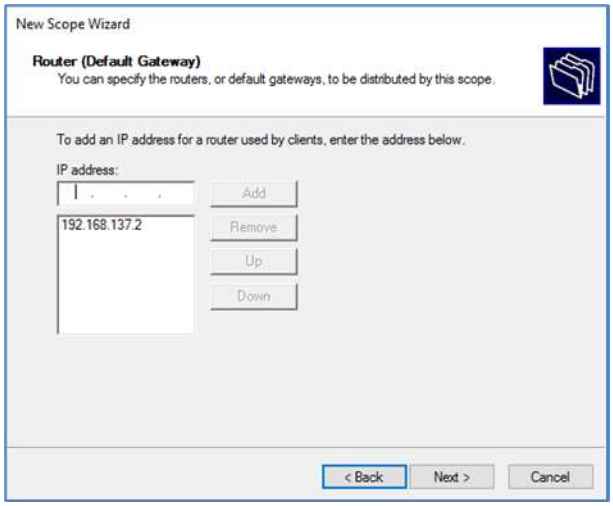
2. Right click IPv4 and pick ‘New Scope’.

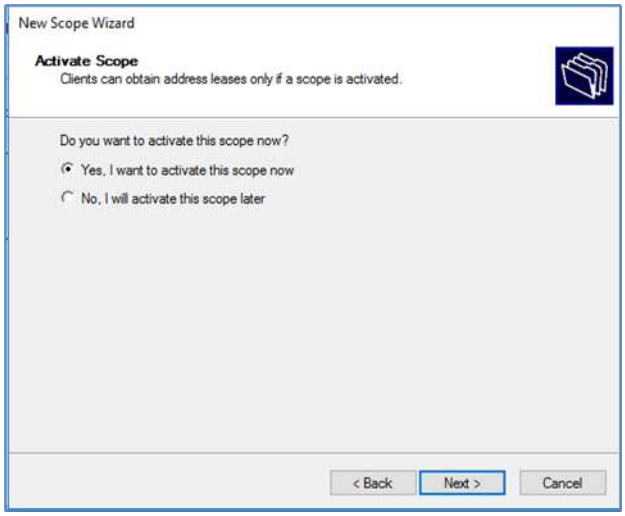
3. Refer to the following to complete DHCP scope:



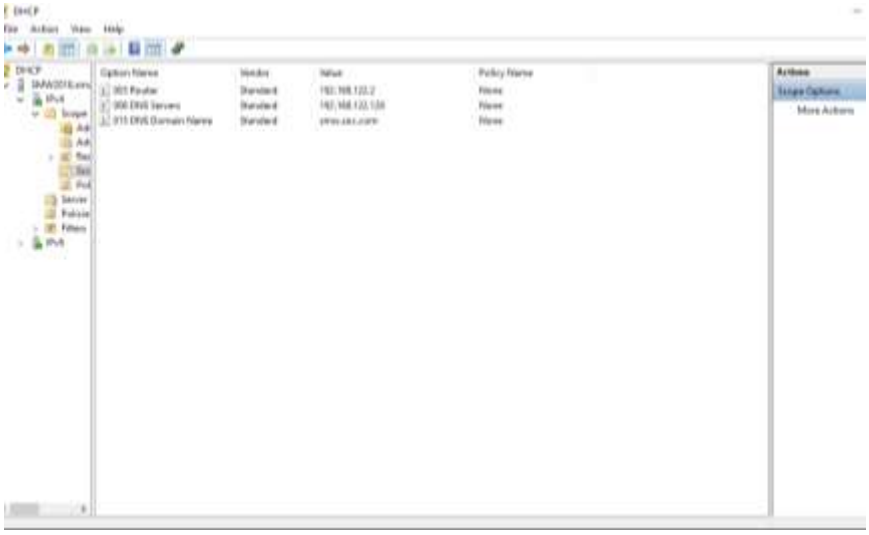

New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address:
192 . 168 . 122 . 100
End IP address:
192 . 168 . 122 . 254
Configuration settings that propagate to DHCP Client
Length:
24
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel


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 DHCPOFFER 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:
Add
Excluded address range:
Remove
Subnet delay in milli second:
0
< Back
Next >
Cancel


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:
Add
192.168.137.2
Remove
Up
Down
< Back
Next >
Cancel



4. You may now verify your scope configuration at the DHCP Manager Console:

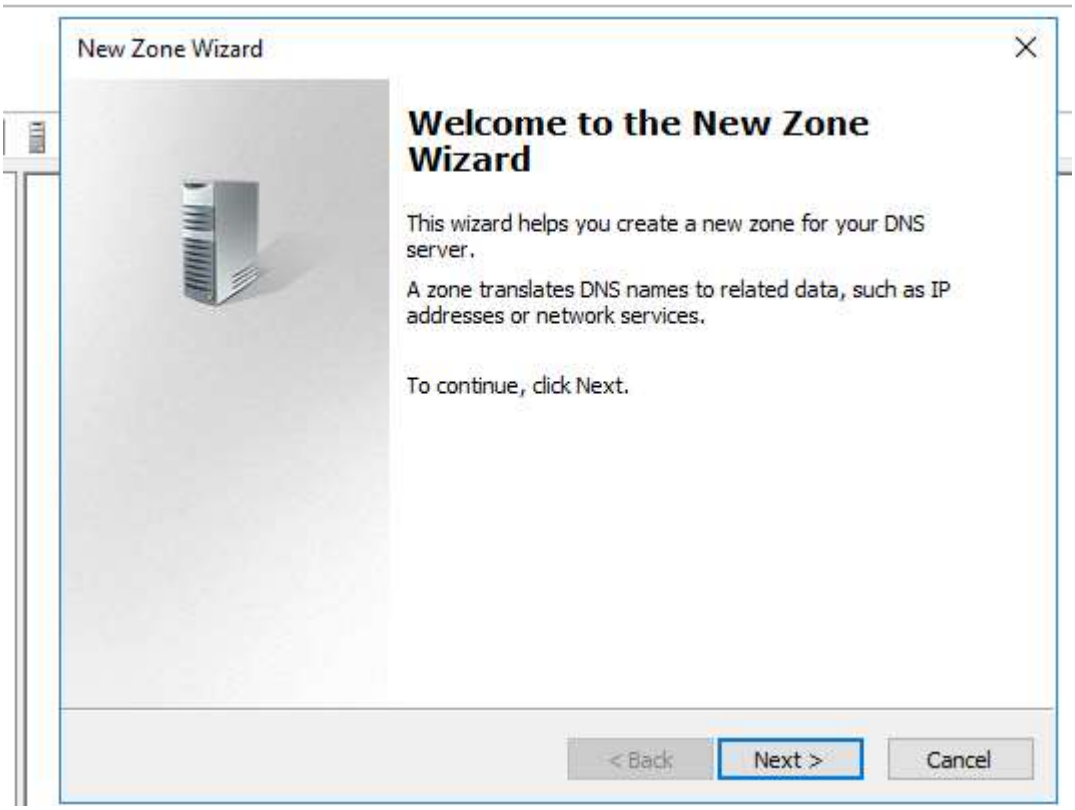


5. You may now close the DHCP Manager console

3.1.5. Setting up DNS reverse lookup record

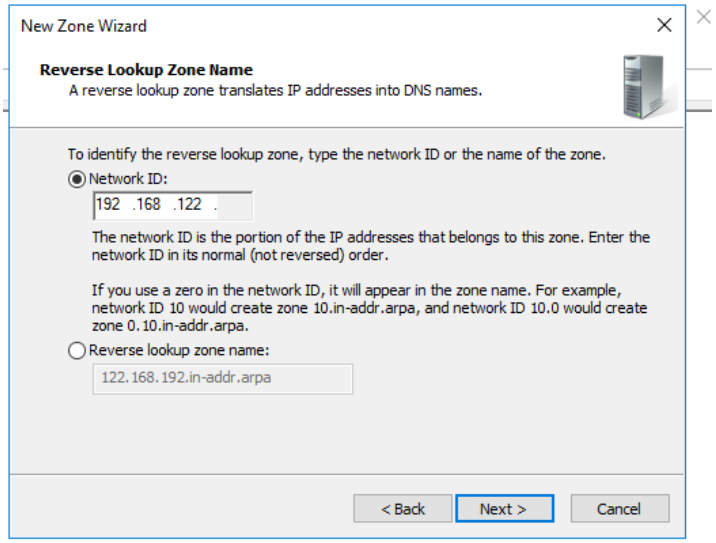
1. Open Server Manager, on the top right click on Tools > DNS.

2. Right click on Reverse lookup zone, select new zone.



3. Take all default values and click next until you reach reverse lookup zone name. Select IPv4 Reverse Lookup Zone.

4.Key in the network ID (first 3 octet of your IP address)



5. Accept the default values and complete the wizard.

6. Once reverse zone is created, you can add pointer record (PTR) of your domain controller into the zone.

7. Under forward zone, click on domain name. Double click on your domain controller name. Check the box ‘Update associated pointer record (PTR)’ click apply and ok.

3.2. Setup for 2nd domain controller

The procedures that follow are for setting up a second domain controller. The second domain controller's job is to make it possible for the high availability arrangement between two domain controllers to continue to function flawlessly even when the first domain controller is offline.

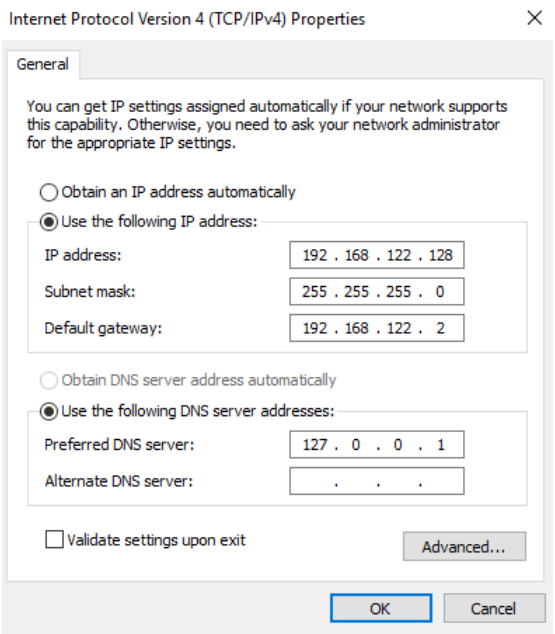
3.2.1. Set the Static IP Address

1. Open 'Network and Sharing Centre by right clicking on the internet icon on the bottom right of the taskbar.

2. Click on "Change adapter settings”.

3. Right click on the ethernet adapter. Select properties.

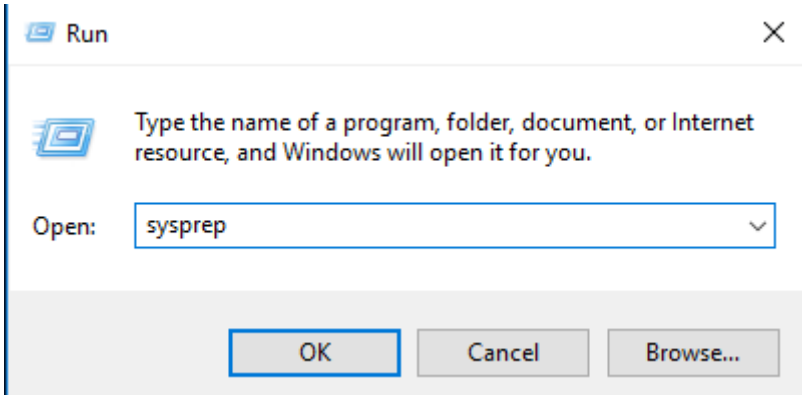
4. Key in the value of your Ip.



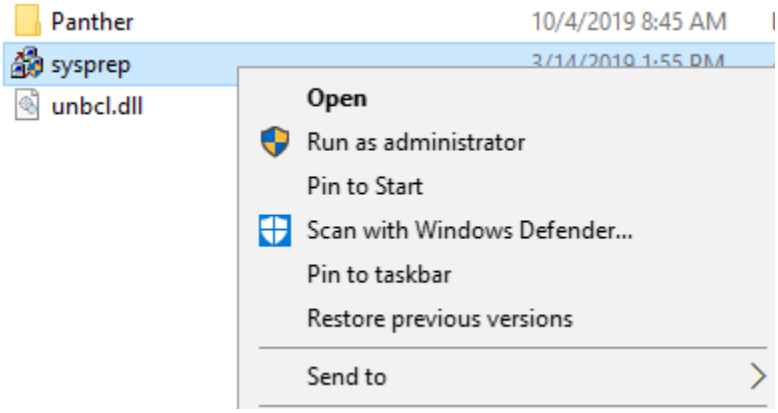
3.2.2. Change the SID

The SID for DC2 will be the same as DC1 because DC2 is a duplicate of DC1. Two machines with the same SID cannot coexist in the domain according to Active Directory. We must modify the SID on DC2 in order to enable OC2 to join the domain. The SID must be changed as described below for the machine to join the domain.

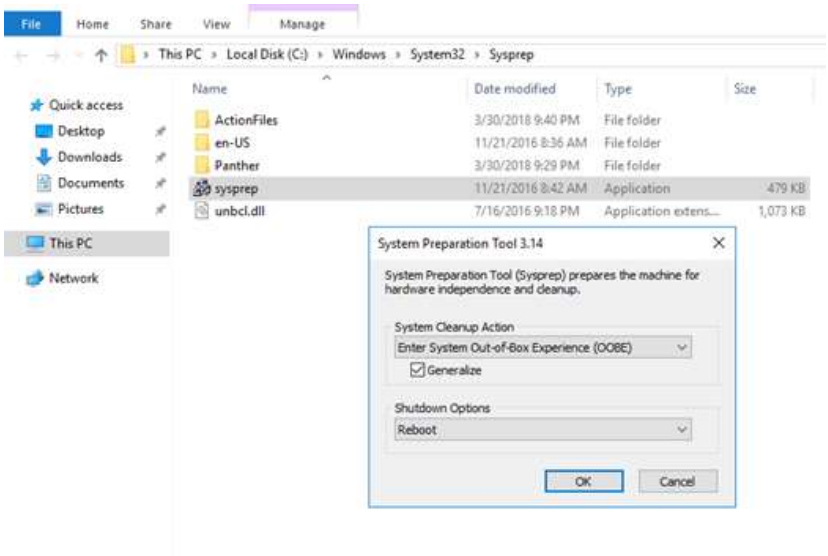
1. Right click on Windows button, select 'Run' and enter in 'sysprep’



2. Run the sysprep application as administrator



3. Choose the default option with tick.



4. Change your administration password and click finish

5. Once the system is rebooted, you need to change the computer name has it has been assigned with random value

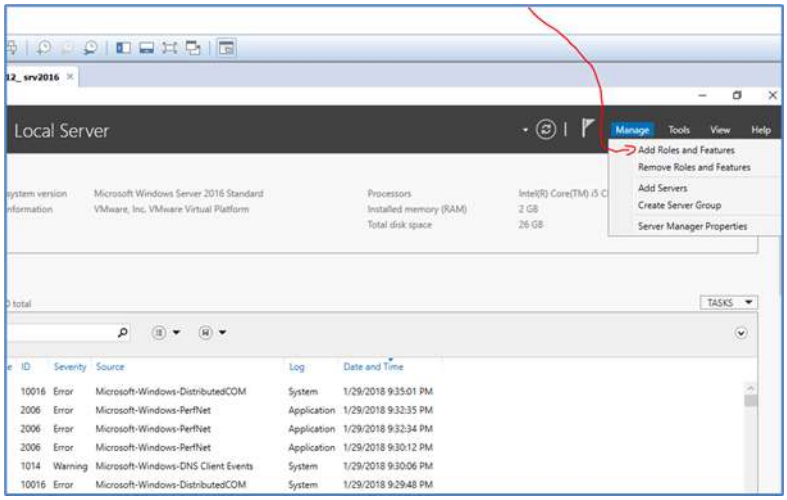
6. Click on computer name

7. Click on ‘Change’. Rename Computer name. You will be prompted to restart your computer. Restart your comp to take effect.

3.2.3 Installation of ADDS

The steps below are on installation of ADDS to make it a domain controller.

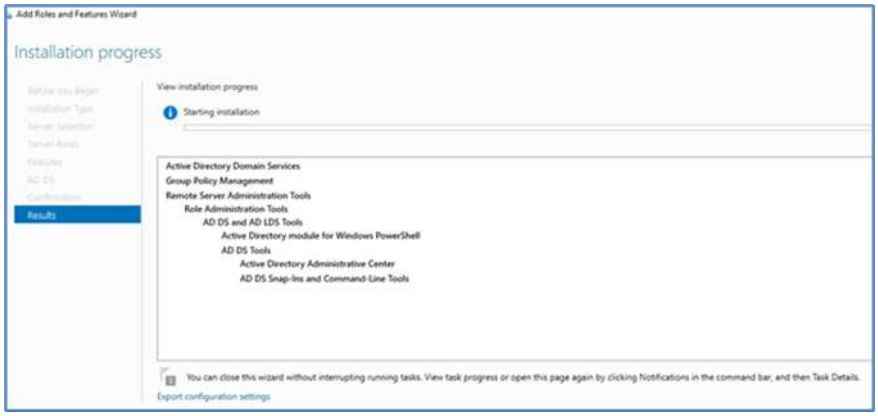
1. To add ADDS role: At server manager, on the top right click on Manage Add roles and features. (Ensure that you have internet connection after having setup a static IP address)



2. Click next. Select `Role-Based or feature-based installation`. Click next.

3. Under Server Selection, select 'Select a server from server pool and select your server. Click Next.
4. Under server roles, select "Active Directory Domain Services. A pop up will appear and select 'Add features' Click next.

5. Accept all default options given and click next till the installation page and click install. (Image below shows the installation of ADDS)

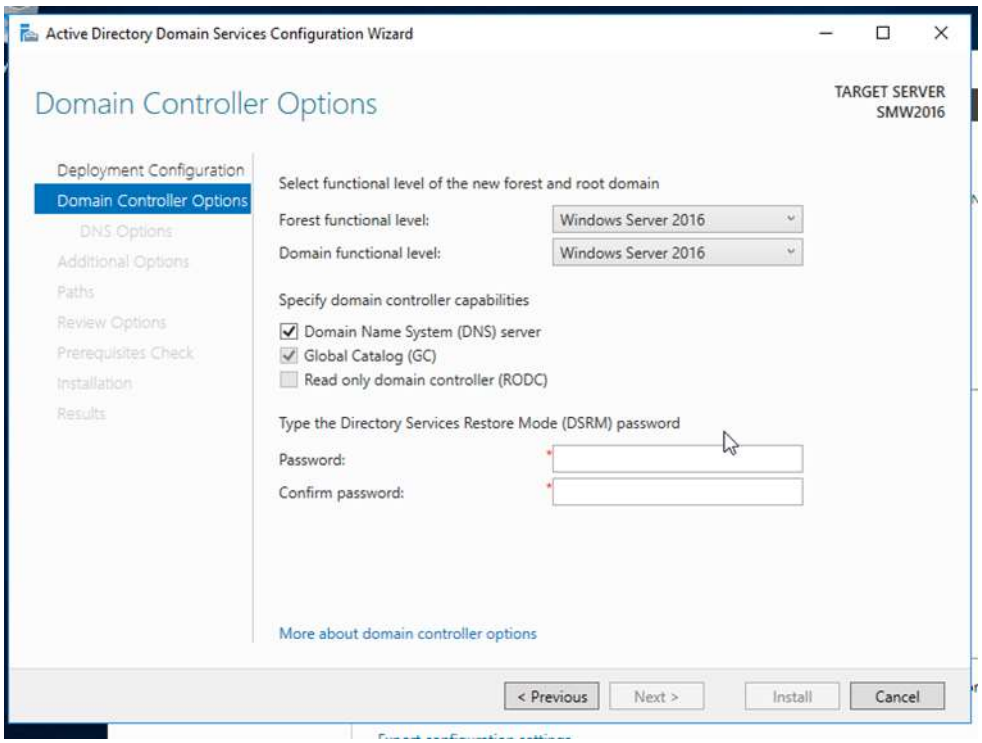


6. After installation is completed, we need to add the DC 2 into existing domain of DC)

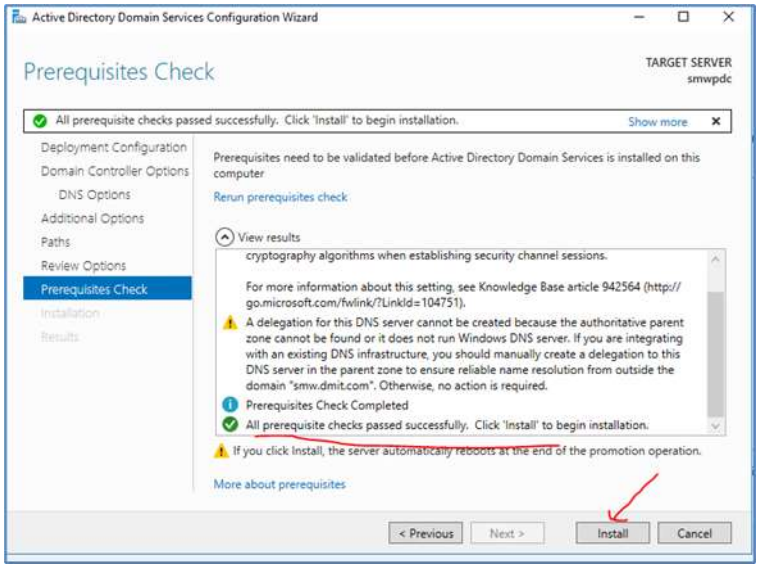
7. A configuration wizard to promote server to domain controller will pop up.

    a. Click 'Add a new forest' and insert a root domain name.

8. Click next forest and domain functional level as set at Windows Server 2016 Ensure Domain Name System (DNS) server clicked. Provide a password. Click next.



9. Take the default options for DNS options and Additional Options and Path
10. Review your options. To proceed, click next
11. You may begin to install if the prerequisites check is successful.



12. After the installation is completed, your server will automatically restart if it does not, manually restart your server You would your domain name is configured under local server.

3.2.3. Joining the domain in DC1

1. Press the flag on the top right of server manager. Click ‘promote this server to a domain controller’.

2. Choose ‘Add a domain controller to an existing domain’. Specify your domain name and key in the credentials of the domain administrator in DC1.Click next.

3. Accept the default options and provide a password. Press next.

4. Accept the default options in DNS options. Under, additional options, select DC1 from ‘replicate from’. Click next.

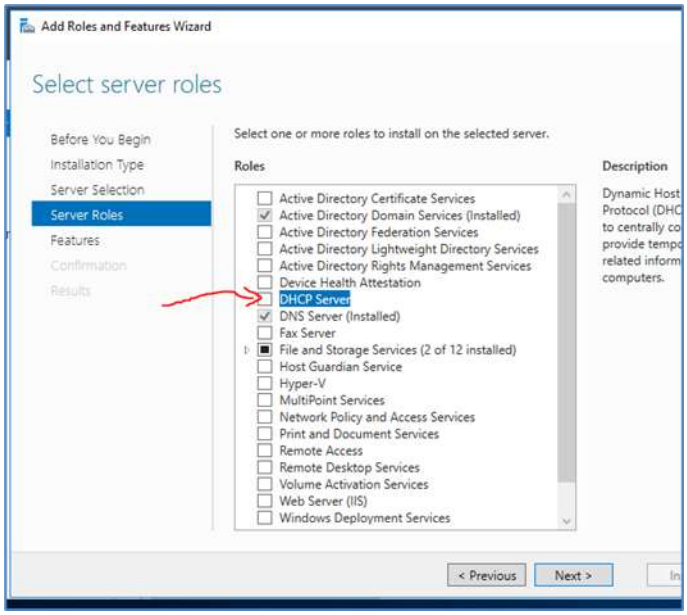
5. Accept the next few pages default values and click next until you are at prerequisites check page. If prerequisites check is successful, proceed to install. After installation, your computer will be prompt to restart automatically.

3.2.4. Install DHCP Service

This section covers an installing DHCP. To provide Dynamic IP address to client that is connecting to the network

1. Click on Manage Add Roles and features.

2. Select the default options until you are at Server roles page. Select ‘DHCP Server’ and Add Features



3. Accept all default settings and install DHCP server

4. After installation, you are still required to complete the post-deployment configuration by clicking on the top right-hand side of server manager.

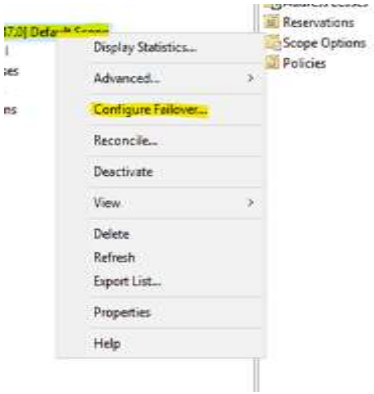
5. Accept all the default options and click connect.

4. Synchronization between two domain controllers

4.1. Configuring DHCP failover on DC1.

1. On Server Manager, Click on tools = DHCP

2. Right click on your scope and select ‘Configure failover’.



3. Add your DC2 Ip address as your partner server and click next.

4. Select `modes` for load balance and provide a password. Click next.

5. On DC2, you can see that the failover is in effect by going into the properties of scope.

6. To allow client to do lookup when receiving IP from DC2, we need to add DC2 IP address
to DNS server under DHCP scope option.
7. Open DHCP > Your scope> Scope Options.

8. Double Click on ‘006 DNS Servers’ Add DC2 IP address in and click Apply.

4.2. Replication of sites

1. On DC1, Open command prompt as administrator. Type `repadmin /replsummary` This is to view the replication state and the health of it.

2. To check the replication status and the most recent attempt to implement an inbound replication of Active Directory partitions by the specified domain controller, type repadmin /showrepl in the command prompt. Finding out the replication topology and replication failure is made easier by it.

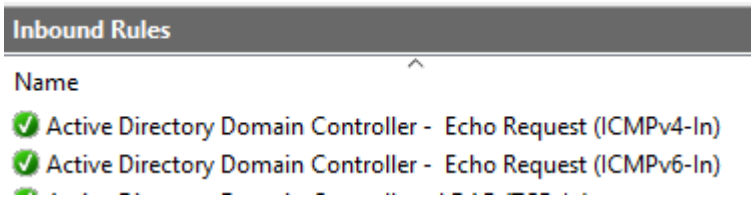
3. To perform a pull updates from DC and pull replies from 2016, type "repadmin /syncall SMW2016 /AeD."

4. To perform a push replication, enter "repadmin/syncall SMW2016/APED," which will send updates from DC1 to other DCs.

5. Firewall Security Settings

1. Open Server Manager Click on Tools> Windows Firewall with Advanced Security.

2. Click on Inbound Rules. Right click ‘Active Directory Controller -Echo Request(ICMPv4 In). Click on properties.



3. Click on ‘Scope’ tab and click on “These IP address” under remote Ip address. Click Add.

4. Click ‘Predefined set of computers’ and select ‘Local Subset’.

5. Select ‘OK’ and apply

6. Repeat the steps on your Domain Controller

6.DNS High Availability

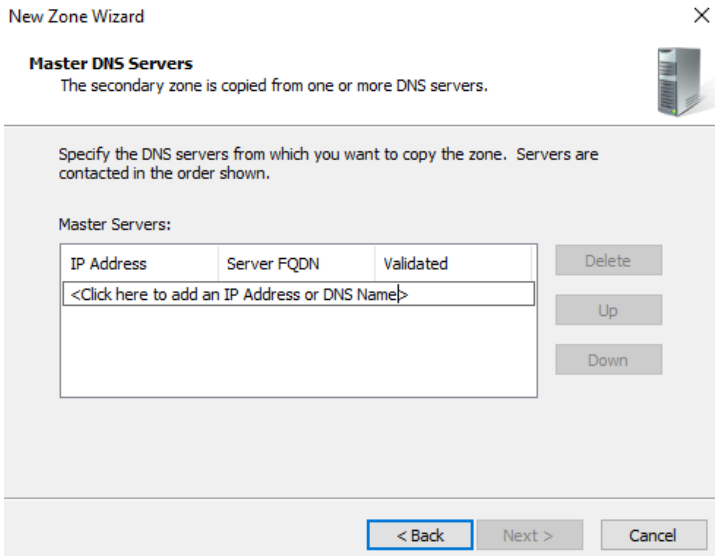
6.1 Setup of a secondary DNS server.

1 Under DC2, go to server manager, click on Tools > DNS
2. Right click on forward lookup zone> New zone

3.Click next and select secondary zone

4. Click next and type in domain name of DC1 as your zone name

5. Click next and type in the Ip address of DC1



6. Go to your DNS on DC1. Right click on your domain name and click on properties.

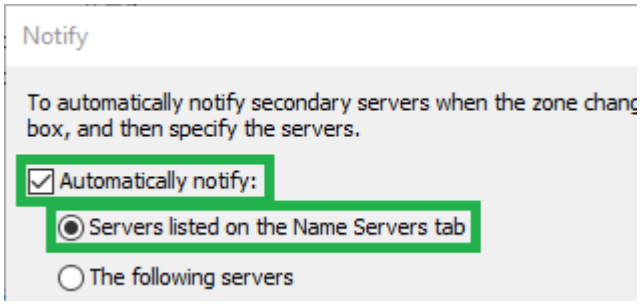
7. Click on zone transfer. Tick ‘Allow zone transfers’ and select ‘Only to servers listed on the name server tab.

8. Click on ‘Name servers tab. Click add

9. Add your DC2 Ip address and click ok

10. Click on zone transfer tab and click on notify

11. Tick `automatically notify` and with servers listed on the name server tab. Click ok after you are done



12. Refresh the page after a few seconds it is done transferring and your DNS from DC1 will appear

6.2. DNS on ethernet adapter not having loopback address.

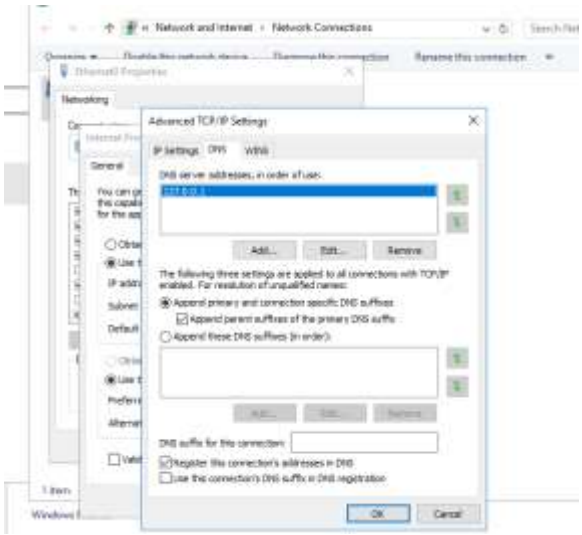
Active Directory could be unable to locate its replication partners if the loopback IP address is listed as the initial DNS server. The performance and availability of DNS servers are improved when each DNS server has its unique IP address included in the list of DNS servers.

1. Open Network and Sharing Centre by right clicking on the ethernet icon on the bottom right of the taskbar and click on 'change adapter setting.

2. Right click on the ethernet adapter and click on properties

3. Click on `internet protocol version 4(tcp/ipv4) and click on Advanced

4. Click on `Dns` tab and click add



5. Add in loopback address and your DC2 ip address. Rearrange the order of Ip address by DC2, DC loopback.

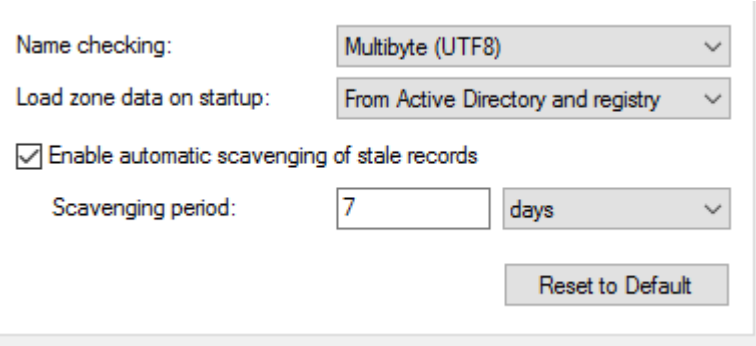
6.3 DNS Scavenging

DNS scavenging should be enabled as the size of the DNS database can become excessive. Scavenging automates the deletion of old DNS records. When scavenging is disabled, the records must be deleted manually, or the size of the DNS database can become too large and will have an adverse effect on performance. (Perform DNS scavenging on both DC1 and DC2)

1. Under Server Manager, Click on Tools > DNS

2. Right click on your domain name and select properties.

3. Go to Advanced tab and click enable automatic scavenging of static records. Leave the values at the default values (7days) Click apply.



6.4 DNS Forwarder

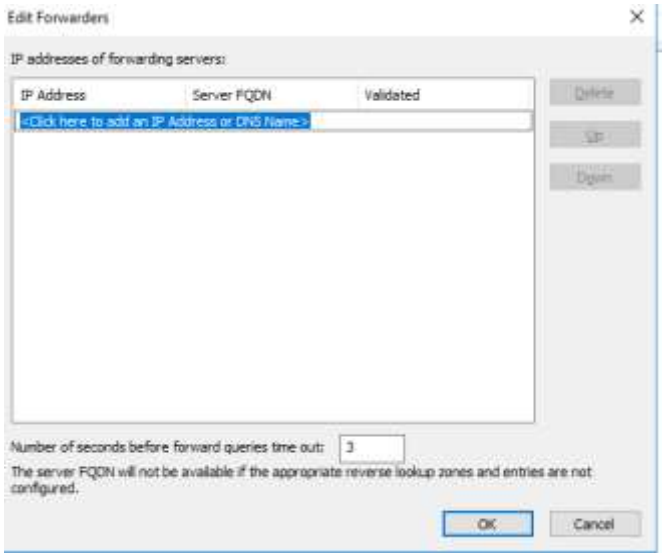
To provide redundancy, it is better to have more than one DNS forwarder. If a single forwarder fails to respond, DNS clients might be unable to resolve DNS queries which could lead to a single point of failure.

1. Under Server Manager, Click on Tools > DNS

2. Right click on your domain name and select properties

3. Click on `forwarders` tab and clicked edit

4. Enter an Ip address of `8.8.8.8` and click ok and apply.



7. Test if a client can join domain

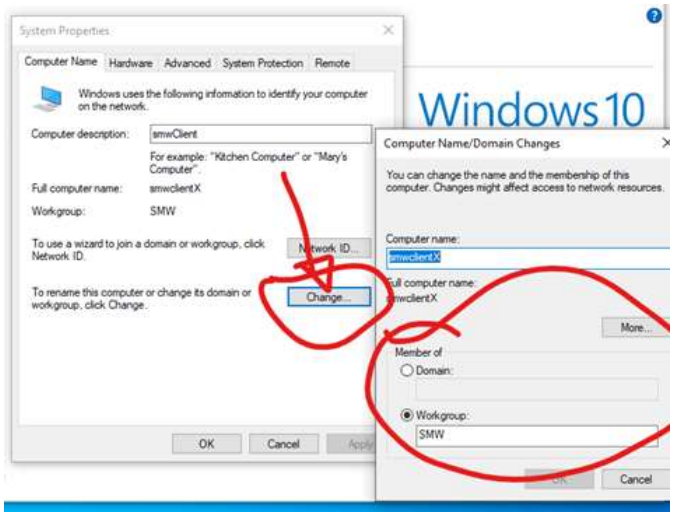
This section covers on how a client can join the domain.

1. Right click on Window Icon and click `system`.

2. On the right-hand pane, click on `Rename this PC` (advanced)

3. Click on change

4. Click on domain option and enter your domain name. Press "Ok" Provide your domain administrator credentials when prompt Restart your computer after joining the domains to take effect.



8. Recommendations

Base Computer Specifications

We advise using at least 8GB of RAM on the base computer that is running the images when following the instructions in this report. This is due to the configuration's requirement that at least 3 images be used; occasionally, more than one image must be running at once. Therefore, 8GB of RAM is the required minimum, but 16GB is advised.

Turning off Windows Auto Update

Windows Auto Update would be another setting that could be changed for convenience. To ensure that everything goes smoothly, we want to keep the number of breaks between steps to a minimum while carrying out this practical. Therefore, we should disable Windows Auto Update in the Group Policies when making the configurations described in this report. However, given that updates are crucial for the security of systems, we advise turning it back on after configurations have been made.

9. Demonstration Agenda

1. Replication of ADDS

- Show that the “Assignment” OU created is replicated for both Domain Controllers
- Add a user and show that user is replicated.

2. DHCP Failover

- Run ipconfig on client with Primary Domain Controller (192.168.37.10) DHCP on
- Turn off DHCP service on Primary Domain Controller (192.168.37.10)
- Show that Secondary Domain Controller (192.168.37.11) is now DHCP server.

3. Secondary DNS Server

- Ping google.com on client with Primary Domain Controller (192.168.37.10) on
- Turn off Primary Domain Controller (192.168.37.10) DNS
- Show that client can still ping google.com.

4. Show if Primary Domain Controller is down

- Restart the client.
- Run ipconfig to show Secondary Domain Controller (192.168.37.11) is the DHCP server.
- Show that client can still ping google.com

10. Conclusion

This report summarizes the procedures and factors to take into account when setting up a domain network with high availability features. In order to accomplish this, we have used two domain controllers, with the secondary domain controller set up as a failover server in the event that the primary domain controller goes down. It is wise to learn how to configure a network with high availability because doing so has many benefits, including improved disaster recovery and increased reliability.

11. Reference

Practical 1

Practical 4

Practical 5

Bionda, E. (2020). *How to configure DHCP failover*. [online] BlueCat Networks. Available at: https://bluecatnetworks.com/resources/how-to-configure-dhcp-failover/ [Accessed 9 Feb. 2023].

Beer, J. (2018). Configure Secondary Zone – Windows Server 2016. [online] 18 May. Available at: https://www.readandexecute.com/how-to/server-2016/dns/configure-secondary-zone-windows-server-2016/ [Accessed 9 Feb. 2023].

Deland-Han (n.d.). *Configure a secondary name server - Windows Server*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-secondary-name-server [Accessed 9 Feb. 2023].

Allen, R. (2018). *Repadmin: How to Check Active Directory Replication*. [online] Active Directory Pro. Available at: https://activedirectorypro.com/repadmin-how-to-check-active-directory-replication/ [Accessed 9 Feb. 2023].

Archiveddocs (n.d.). *Repadmin -replsummary*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc835092(v=ws.11) [Accessed 9 Feb. 2023].