**Secure Microsoft Windows**

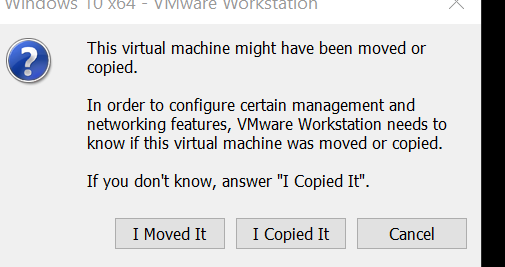
**Practical 1**

**Introduction to SMW Lab Setup and Basic Windows Server 2016 configurations**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   1. Maintain and personalize your own Windows Server 2016 and Windows 10 VMWare Images in the Lab setup. 2. Use Server Manager to perform “add Features” and “add Roles” functions. 3. Set up a simple Domain Controller Server with one client workstation. 4. Set up the DNS Service and DHCP Service in the Primary Domain Controller |

Lab Prerequisites:

* You need to have the text book for your reference.
* Take note that due to VMWare access right issue, you cannot use the Lab PC to do your practical.
* You need to download the VM images to your laptop in order to proceed.
* Keep a copy of your original download, as you will need to use them to clone more VMs in the future labs.
* For the VMware software, you are recommended to use VMware workstation 15.0 or later
* When you are being prompted for the following while powering on a newly copied windows VM.

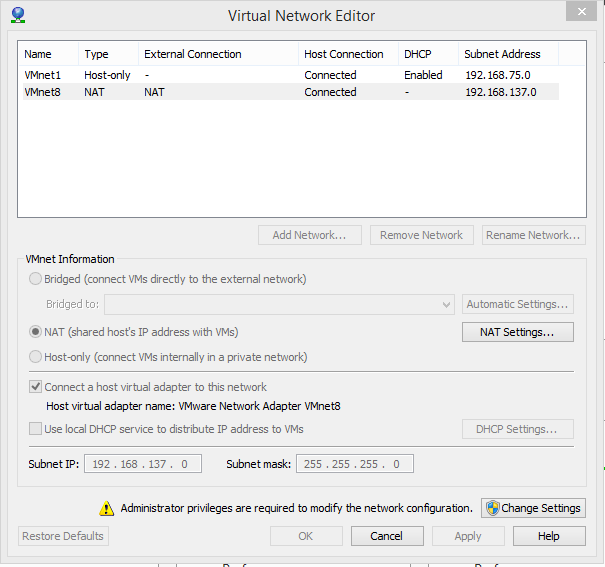


Always answers with 'I Copied It'.

* Be reminded to record down all the important configuration information of your VMs.
  + Passwords, IP configuration, Domain Name, Machine Name, etc …

**Lab exercise 1-0: Understanding the VM Virtual Network Configuration**

1. Start VMware Workstation. Go to Edit, Virtual Network Editor.
2. Select VMnet8, which is the NAT virtual network adapter.



1. Take note of the Subnet IP (circled in red above). When you start up a VMware image with NAT, VMware will assign an IP address from this range to the image.

- Initially, check the 'Use local DHCP service to distribute IP address to VMs' option.

- Once the initial testing is completed, and you are having your own DHCP Service running, you 'MUST' uncheck this option. (All your SMW lab client VMs should use DHCP service offered by your Primary Domain controller, all your SMW lab server VMs should use appropriate static IP settings)

**Lab exercise 1-1: Basic Virtual Machines Setup**

Windows Server 2016

(Domain Controller ) with ADDS, DHCP and DNS.

Windows 10 (Client)

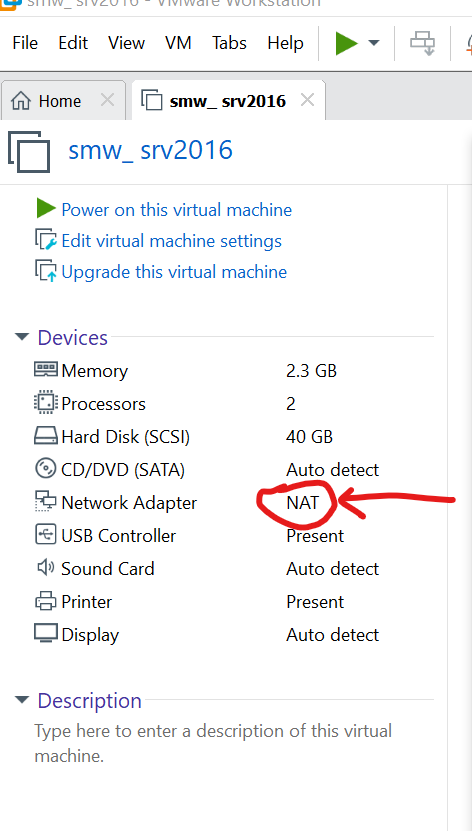
Domain : smw.soc.com

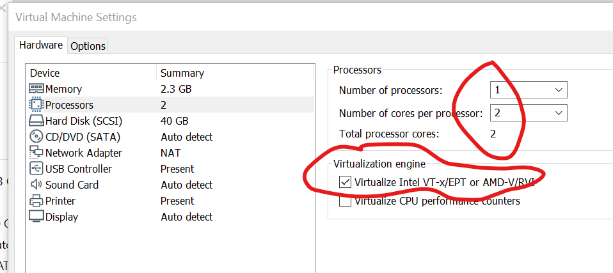
You will be setting up two images. Both images will be part of a domain.

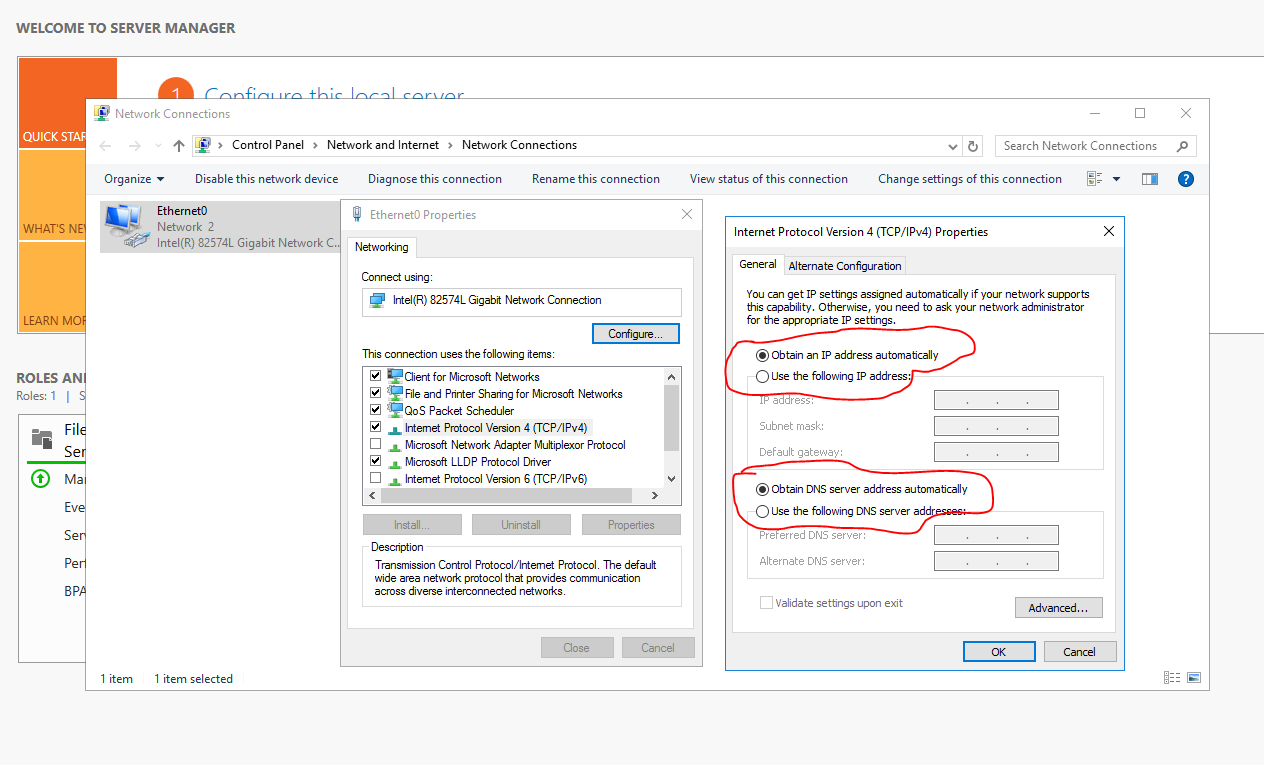
Windows Server 2016 – the Domain Controller and it runs the DNS Service and DHCP Service.

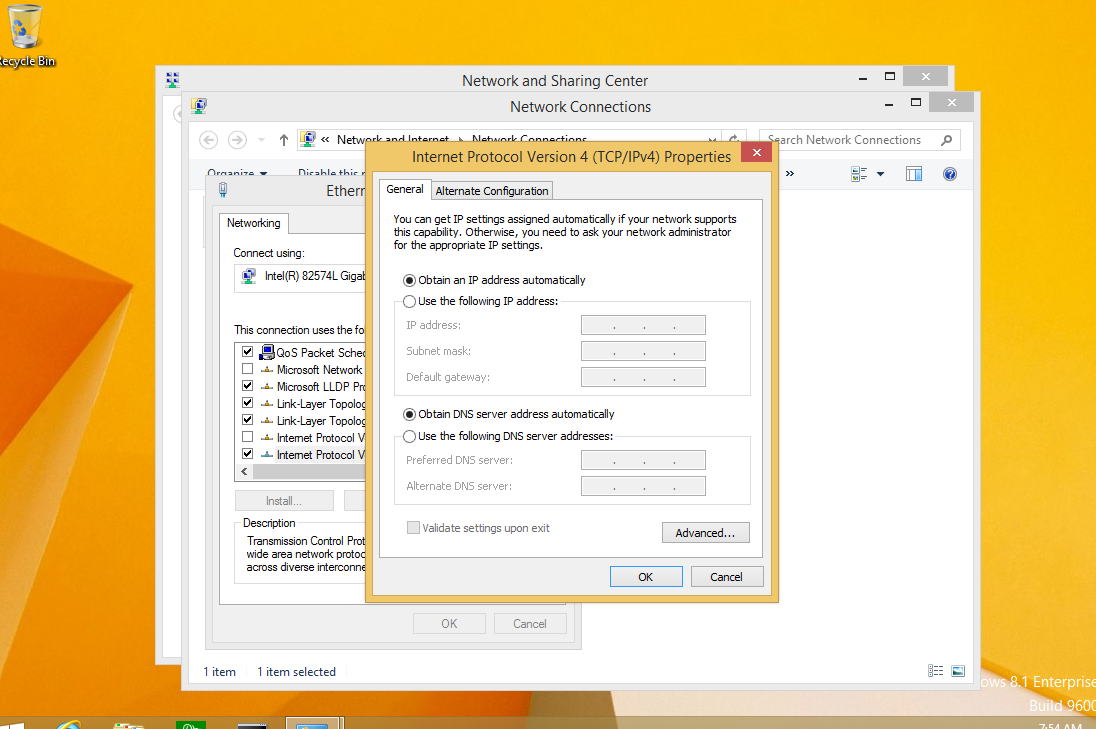
Windows 10 (or you can try with an older version windows 8/8.1) – client

1. Check that the two images in Lab 1 folder (win2k16Std and win10) are using NAT.



1. Check the processor settings of the two images in Lab 1 folder (win2k16Std and win10) to have '2' virtual processors and Virtualization engine on.
2. Power on both images.
3. For the Windows Server 2016 image, to login => (user id : smw\_srv2016 password : 1qwer$#@!)
4. For the Windows 10 image, the local user account ladmin is the Administrator and the password is also 1qwer$#@!.
5. On both images, verify and set the date, time and timezone correctly.
6. On both images, **initially**, set the IP address and DNS Server address to be obtained automatically (using DHCP).





1. On both images, check that you can access the Internet.
2. At this point, for the windows 2016 Server images, modify the IP address, Gateway address and DNS Server to a static value.
   * Your tutor will explain and help you to decide the static values.
   * Hints,: You can use the existing IP settings , except need to change IP address value.
3. Verify again both of the images are able to access the Internet.
4. Record down your windows server 2016 IP settings now:

IP Address:\_\_\_\_\_\_\_192.168.126.90\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Network Mask: \_\_\_\_255.255.255.0\_\_\_\_\_\_\_\_\_\_\_\_\_

Gateway: \_\_\_\_\_\_\_\_\_192.168.126.2\_\_\_\_\_\_\_\_\_

Preferred DNS Server: \_\_\_192.168.126.2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

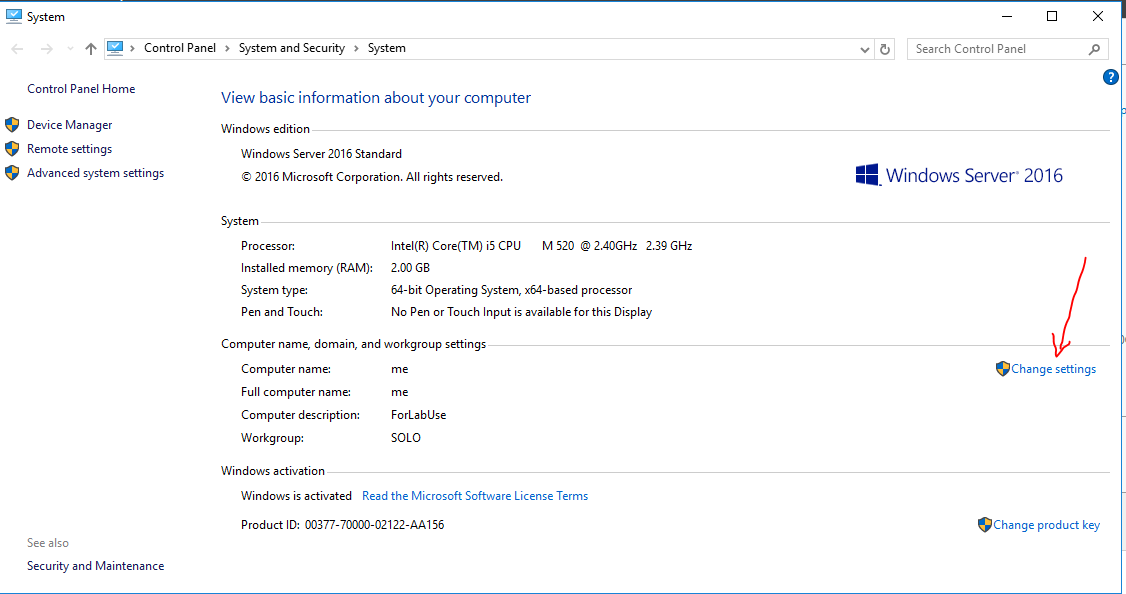
Alternate DNS Server: (can leave it blank)

1. On both images, try to disable the Automatic Windows Update feature (this should be enabled for production systems, but we are disabling it just for a better performance during practical time). However, it may be relatively difficult to figure out how to disable the Server 2016/Windows 10 automatic update feature. If it is so, proceed without changing the setting first.

Caveat: Although we do not want to receive a sudden windows update notification during the practical time it is good to keep you lab VM images up-to-date. Thus, you should manually check for update during the weekends. Fail to keep your VM image up-to-date may cause issues when working on the future lab exercises.

1. On both images, change the computer name. Right-click on Windows button and select System. Under the System menu click Change settings. Click on Change and set a new computer name (anything you like). You will have to restart the image after changing computer name.

Caveat: As we will clone the same VM to create more windows machines in your domain, ensure every VM has its unique and meaningful computer name is one of the important best practices in this module.



Reflection Prompt: Other than the ipconfig /all command, what are the other ways to check the network settings in a Windows system ?

**Lab exercise 1-2: Setting up your own Domain**

You will now install Active Directory Domain Services on your Windows Server 2016 and make it a Domain Controller. As the IP address of the Domain Controller should not be changing, please ensure that you have changed the IP address setting of the Windows Server 2016 to static.

For this step, you do not need your Windows 10 VM to be active, you may shut it down to reduce the loading of your notebook.

1. On Windows Server 2016, check out your network status details and take note of the current IP, Subnet Mask, Gateway IP and DNS Server IP.
2. Ensure you have disable the VM Net NAT Local DHCP service.

In vmware > edit virtual network > uncheck local dhcp for nat box for VM Net 8

1. Now set your Windows Server 2016 to a set of workable static values:

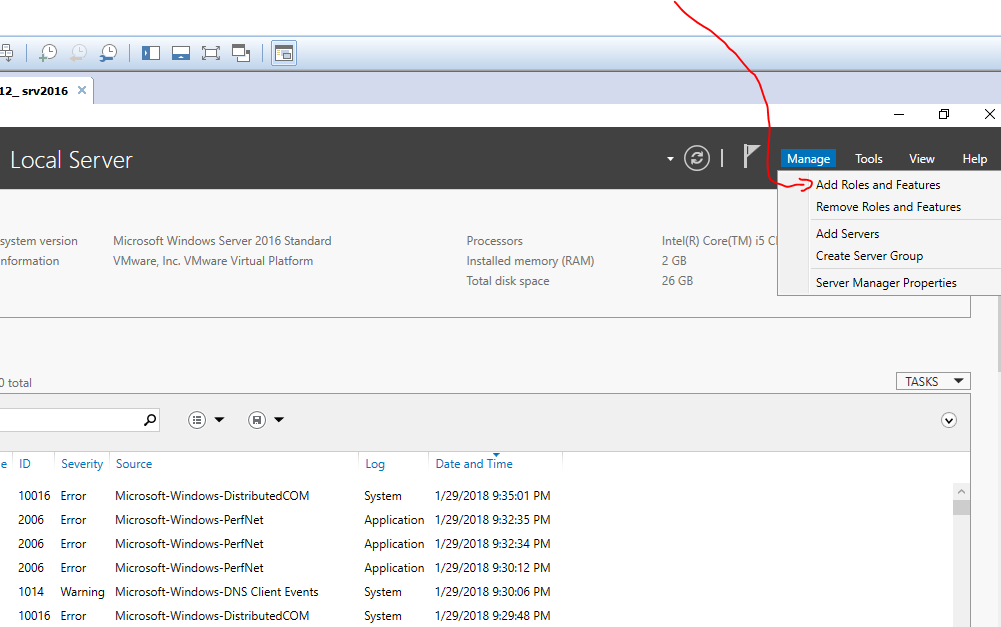
IP address: \_\_\_192.168.126.90\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Net mask: \_\_\_\_\_255.255.255.0\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

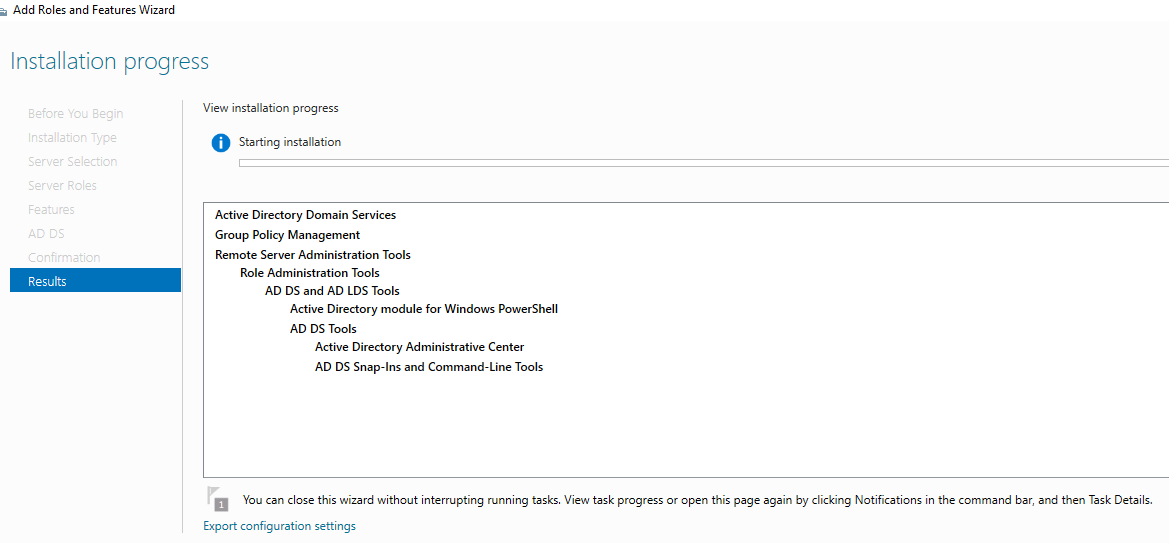
Gateway: \_\_\_\_\_192.168.126.2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Preferred DNS: \_192.168.126.2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

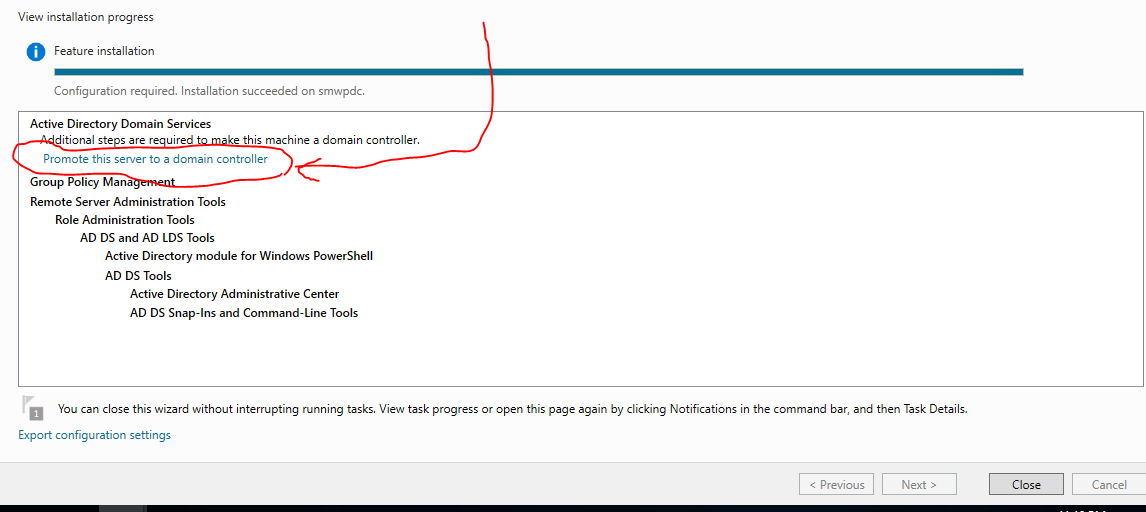
1. Check that you can still access the Internet. Seek for your tutor’s help if it is needed.
2. To promote your Windows server to become a domain controller, add the Active Directory Domain Services role to your server.
   * Try to following the following step by step instructions to carry out this exercise.
     + Refer to your Textbook – Chapter 3 – Activity 1 – Installing Active Directory if needed.
   * To add the role: At Server Manager -> Local Server -> Manage -> Add Roles and Features



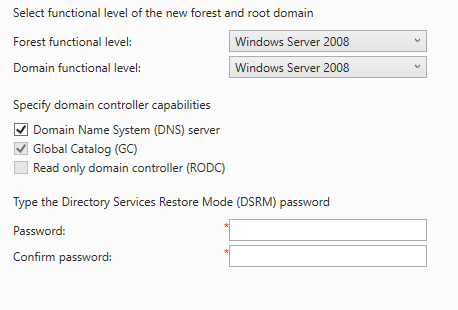
1. Installation in progress:



1. After the installation process is completed, remember to click on the "Promote this server to a domain controller" to proceed to the additional steps:

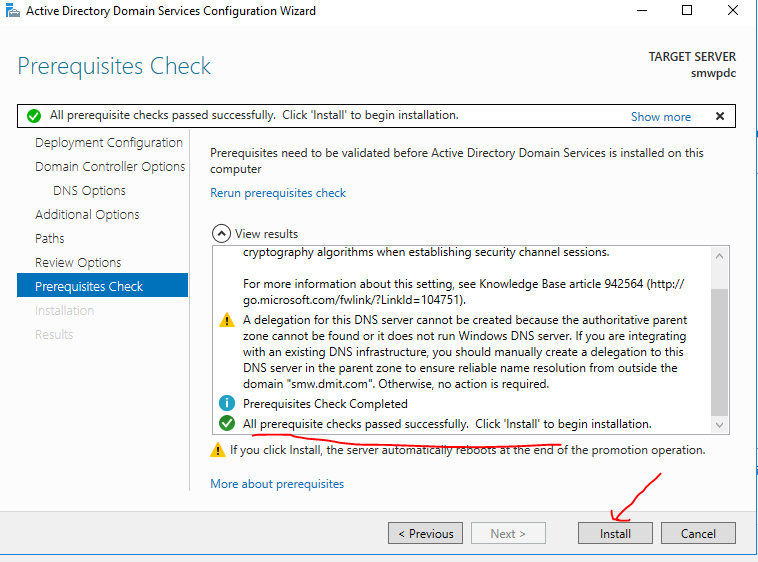


1. Refer to the following to setup your own domain :
2. Deployment Configuration :
   1. Add a new forest
   2. Root domain name (fully qualified domain name FQDN), you can use “smw.soc.com” or any other domain name you like, eg “mydomain.org”. Please avoid to use single word.
3. Domain Controller Option:
   1. Use Windows Server 2008 (Yes, 2008 , not 2012 nor 2016. It is not a typo error.) for both of the Forest Functional level, and the Domain Functional level. You will change them to a higher level in the Lab 2 or Lab 3.
   2. Specify the DNS and the Global Catalog (GC) capabilities.



* 1. For the Directory Services Restore password, you can use : !QWER4321

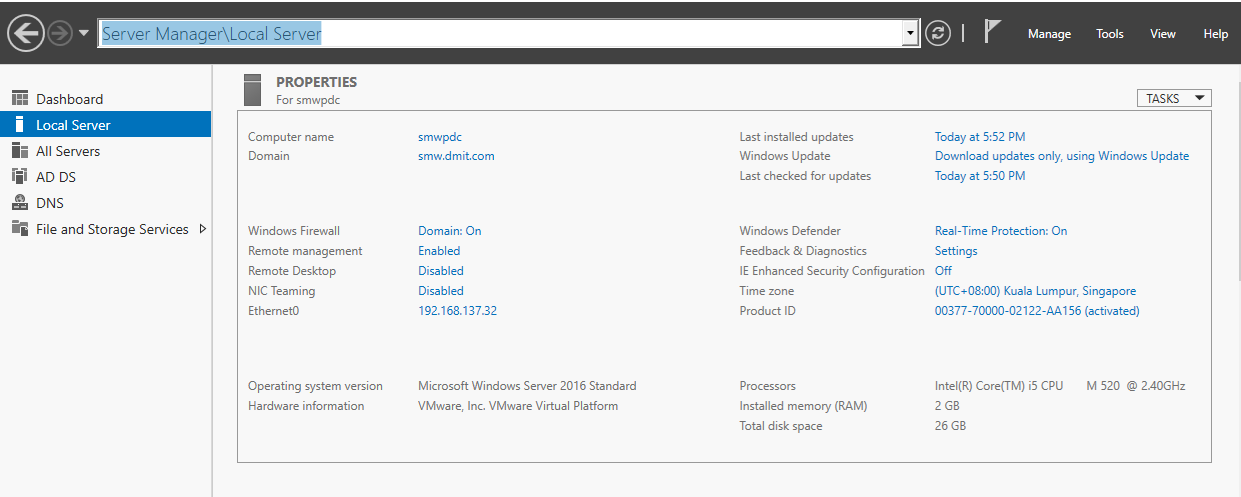
1. DNS Options
   1. You do not need to create DNS delegation as you are setting a Primary Domain Controller.
2. Additional Options
   1. Take the default for the NetBIOS domain name.
3. Paths: Take the default values.
4. Review Options – Examine and verify the options. To proceed, click the next button.
   1. You may try the view script option to learn how to use Powershell script to install a domain controller.
5. Prerequisites Check: (You may proceed if the check is successful, press the install button)



1. When the installation is complete, you will need to restart your server, or it will automatically restart if you have opted for the 'auto-restart if needed' option at the very beginning.

**Lab exercise 1-3: Exploring your Domain Controller**

1. You can login to the server using the same user id : smw\_srv2016 and the same password : 1qwer$#@!
   * Take note that smw\_srv2016 is now promoted to a Domain User account with Domain administrative right.
   * If you are prompted to change your password, please record down the new password!!! (very important)
2. At the Server Manager -> Local Server, explore the properties page:



Click on the Blue color link and explore their functions.

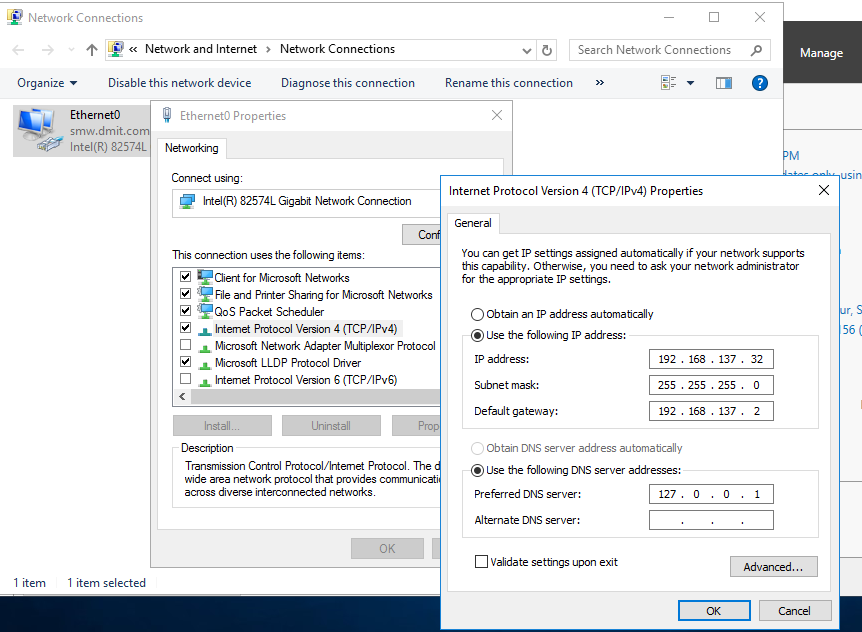
Reflection prompt: Can you identify at least 5 clickable elements in the Server Manager Local server Properties page that are related to the Windows Security measures ? I.e. any misconfigurations/ mis-use of these will cause higher risk of security implications.

Remote Desktop, Windows firewall off, windows defender off

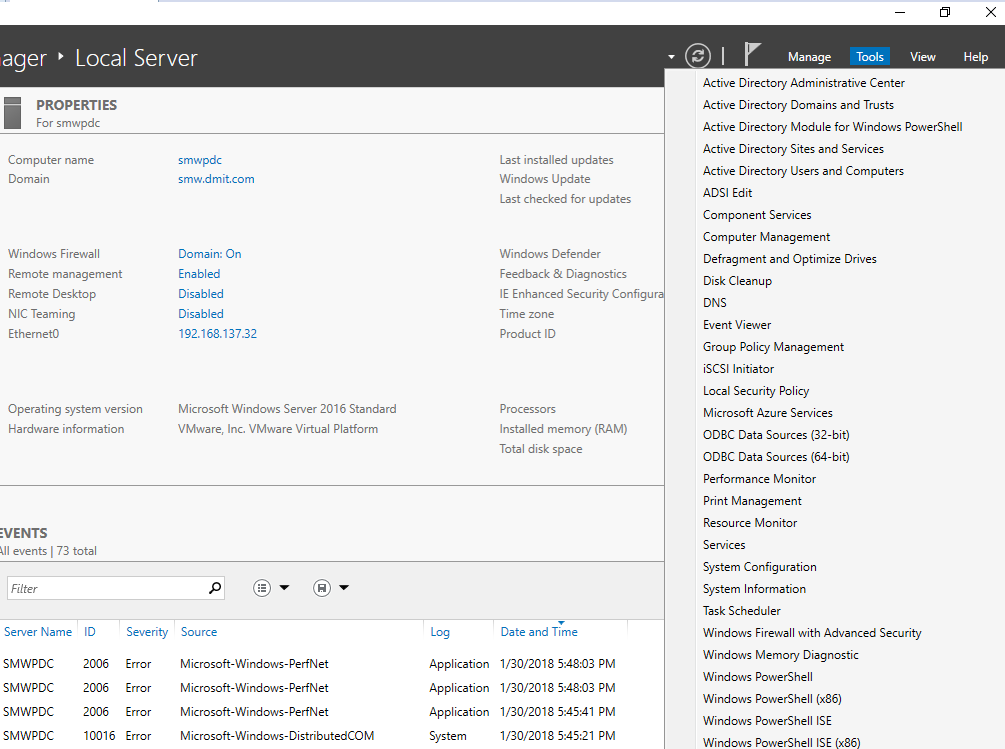
1. At the Server Manager -> Local Server -> Properties

Click on your Ethernet0 ip address to bring up the Network Connections Window.

From there, bring up your current IPV4 network settings Properties Window. Take note that your preferred DNS is now set to 127.0.01. It is because, your server itself is providing DNS service now.



1. Add in your own static IP address as the Alternate DNS server now. This will help to clear the false alarm of 'Not Connected' notification showing at the network connection icon. 
2. At this point, try to access to the web again to verify your current network settings is correct.
3. At the Server Manager -> Local Server -> Tools, explore the following tools:

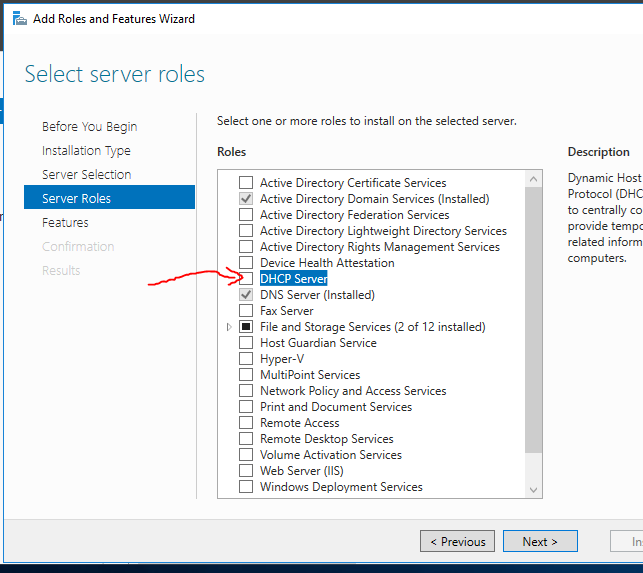


* Active Directory Users and Computers
* Services
* System Information
* Windows Firewall with Advanced Security

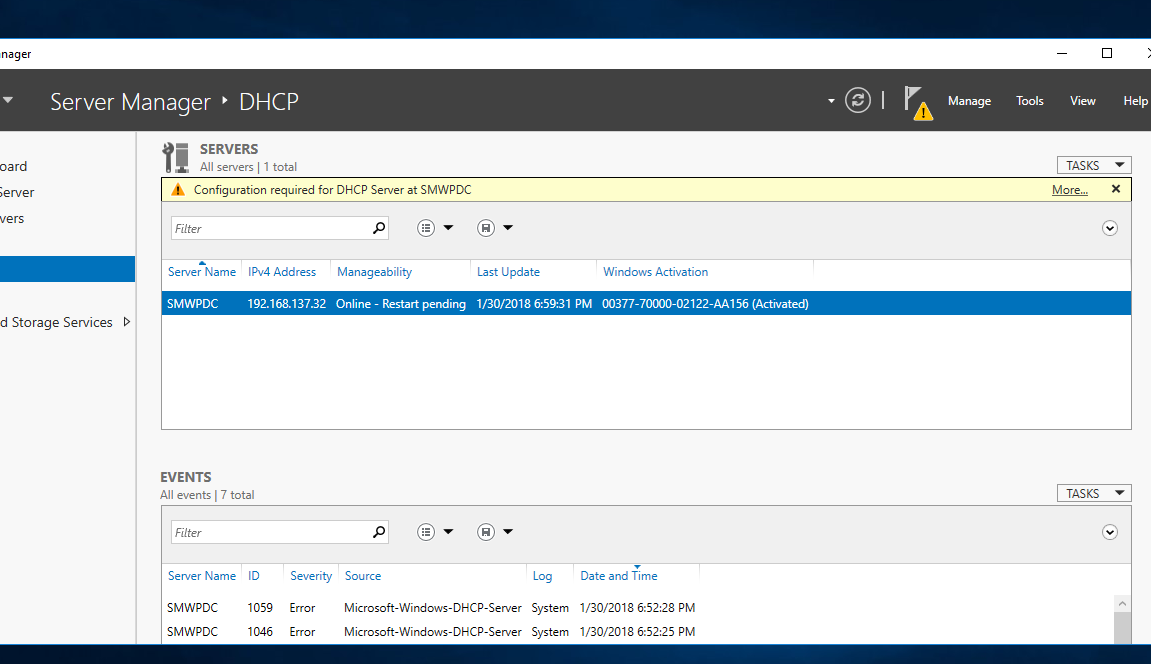
1. Reflection Prompt: Try to run the Group Policy Management Console. From the console, can you find out what is the forest name and domain name of your system?

**Lab exercise 1-4 Adding in DHCP service to your Domain Controller**

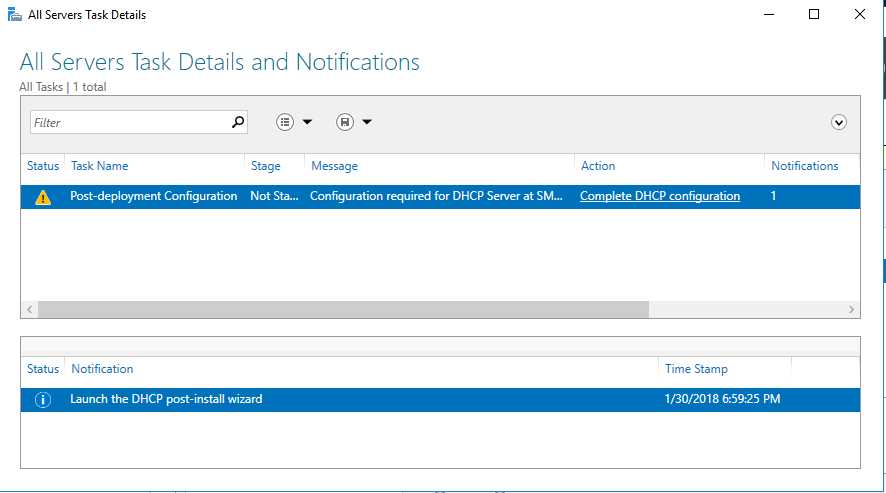
1. Since you are going to run your own DHCP Server for the NAT segment and you have disabled the VMWARE Network Local DHCP service (Refer to Lab exercise 1-2, step 2), there is no DHCP service running in your LAN segment.
2. You need to login to your Domain Controller with an account that is a memer of domain administrator group. You may consult your tutor to find out how to add your smw\_srv2016 user account into the domain administrator group.
3. At the Server Manager -> Local Server, use Add Role feature to add in the DHCP Server role :



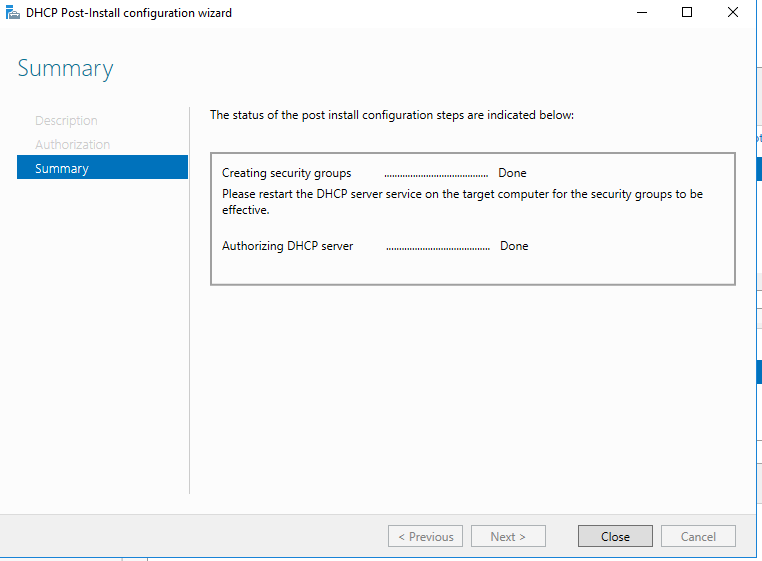
1. You may accept all the default settings and click the next button until the installation is completed.



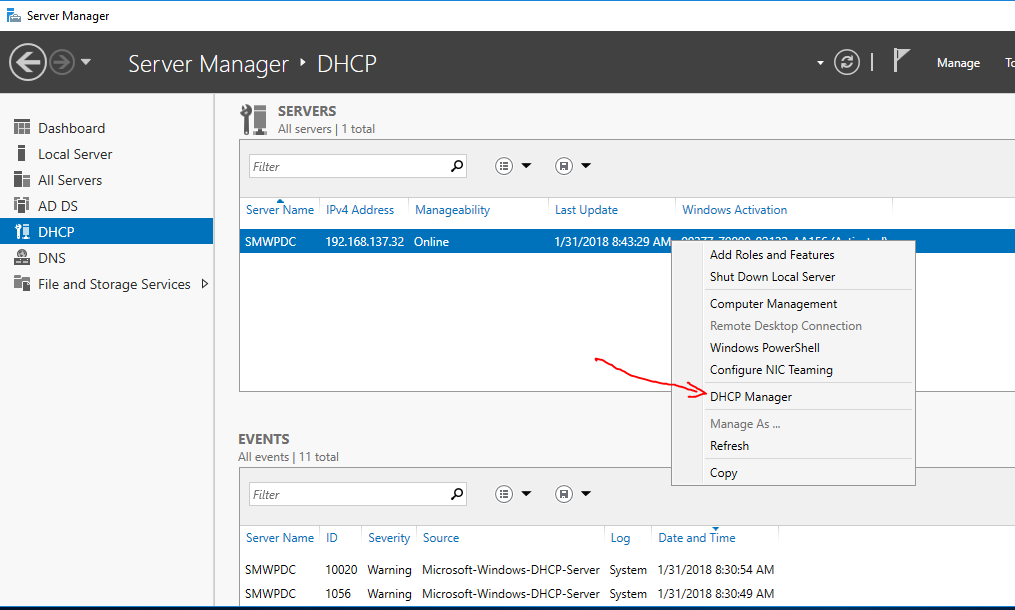
1. After the role and features are added, you still need to complete the required post-deployment configurations.



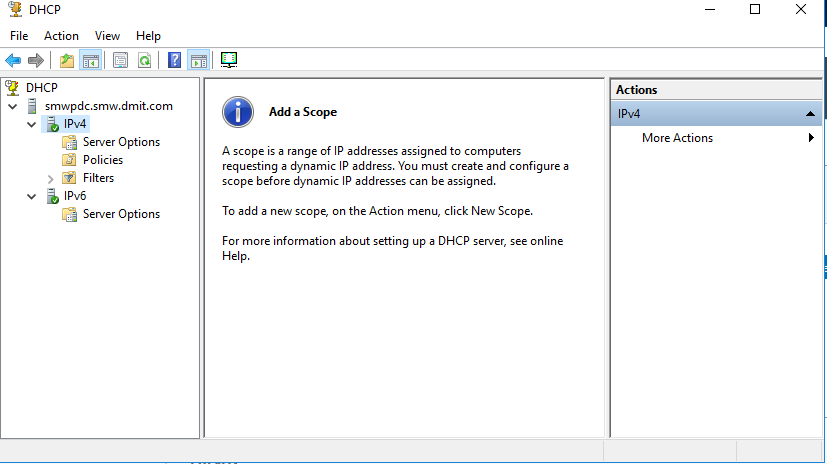
1. Again you can accept all the defaults to complete the post-deployment configuration.



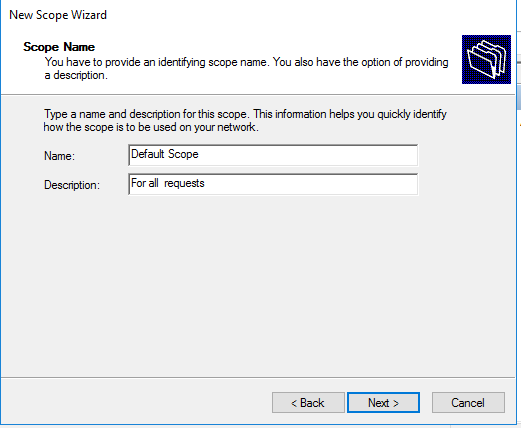
1. The DHCP Scope configuration: The scope definition determines the information to be sent to all connected DHCP clients. You need to start the DHCP Manager to configure the scope.
   1. Access to the DHCP Manager via Server Manager:

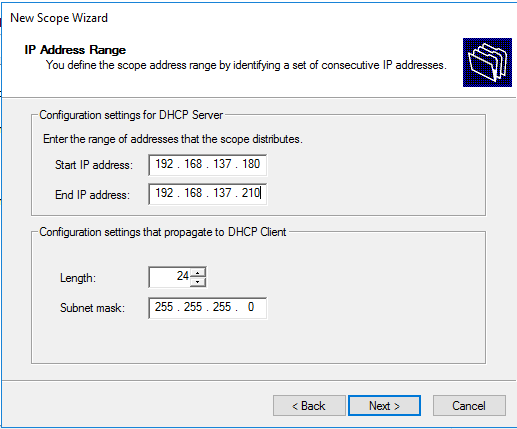


* 1. Adding an active IPv4 scope to provide dynamic address allocation services.
* Right click on the IPv4 node and select 'New Scope'.

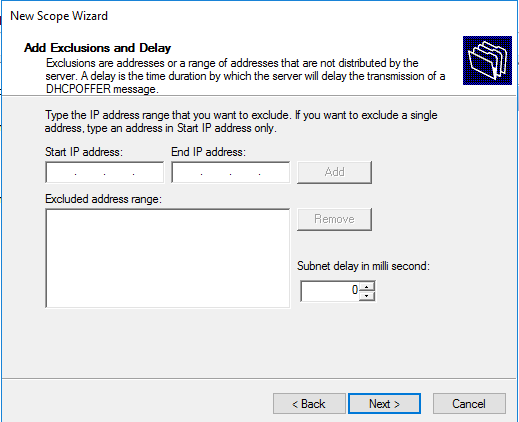


* Refer to the following to complete the configuration guided the New Scope Wizard.



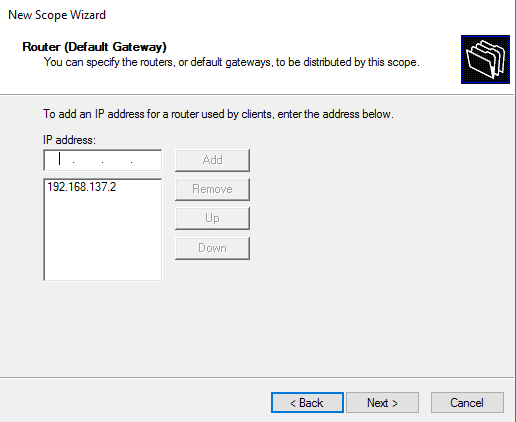


(The IP address range needs to be adjusted to match your VMNet NAT segment settings)

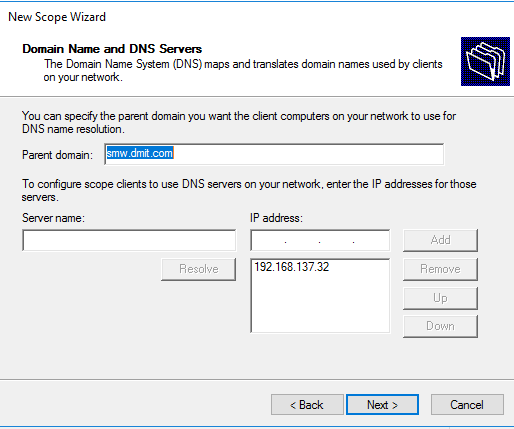


At Add Exclusions and Delay – leave it blank and Click Next to proceed.

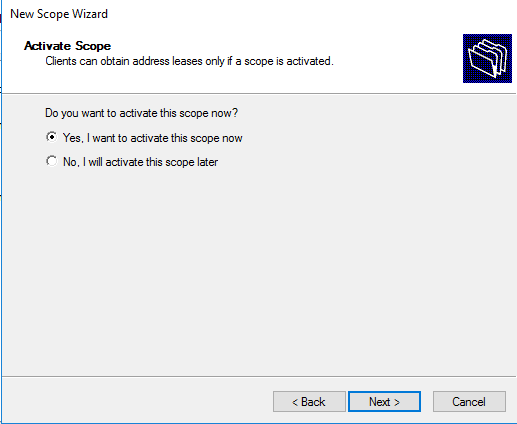
Also takes the default settings for the next two wizard screens until the Router (Default Gateway) screen: You have to enter your VMNet NAT gateway address: in this example, it is 192.168.137.2.



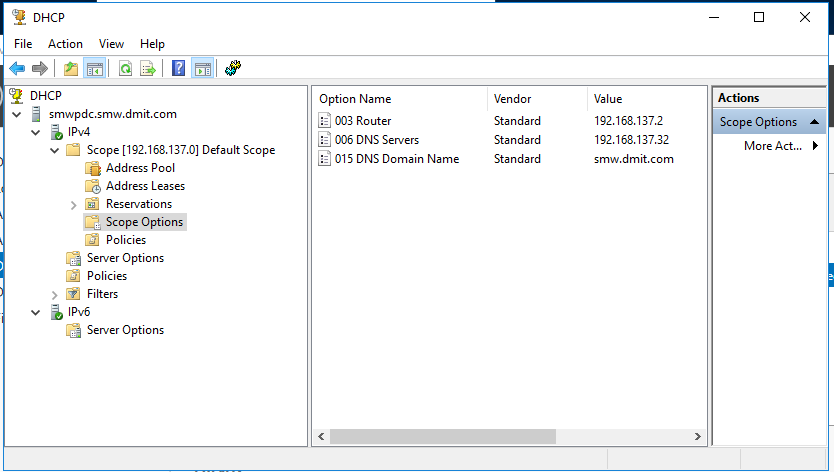
In the Domain Name and DNS Servers screen. Double check if the domain name and DNS server address (It should be your PDC address.) then click the Next button.



You can skip the next WINS Servers screen and reach to the following Activate Scope screen: You may select Yes, and click the Next button to complete the scope configuration.



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



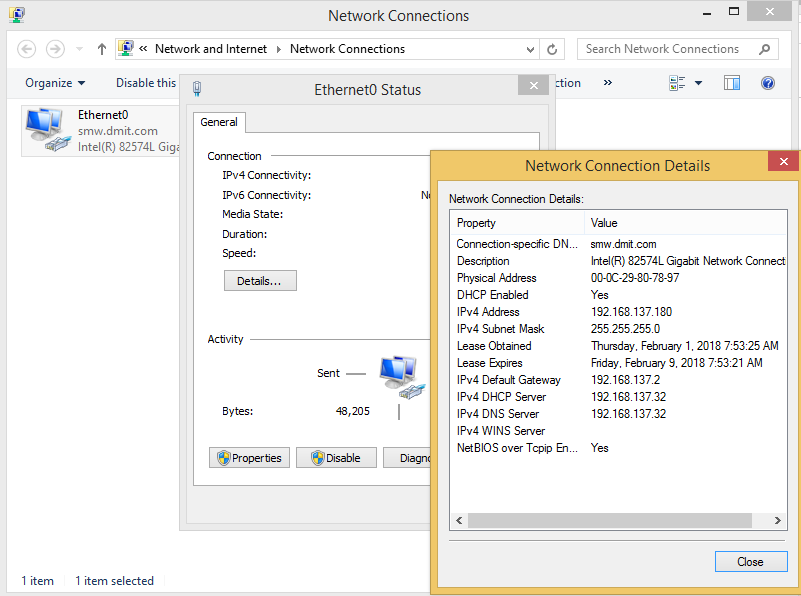
* 1. You may now close the DHCP Manager console and proceed to the next exercise.

**Lab exercise 1-5 joining a client to your domain**

You will now configure your Windows 10 (or Windows 8.1) VM to join your domain.

1. Ensure your Server 2016 is up and running, the local DHCP service of the VMNet has been disable.
2. Start your Windows 10 VM (also connect to NAT segment)
3. Verify the IP settings of the Windows 10 VM remains as dynamic.
4. Check that you can still access the Internet.
5. Verify and record down the IP address, Gateway, and DNS settings of the Windows 10 by using the GUI approach:

At Network Connections->Right Click on the Ethernet0->Click Status->Click Details..



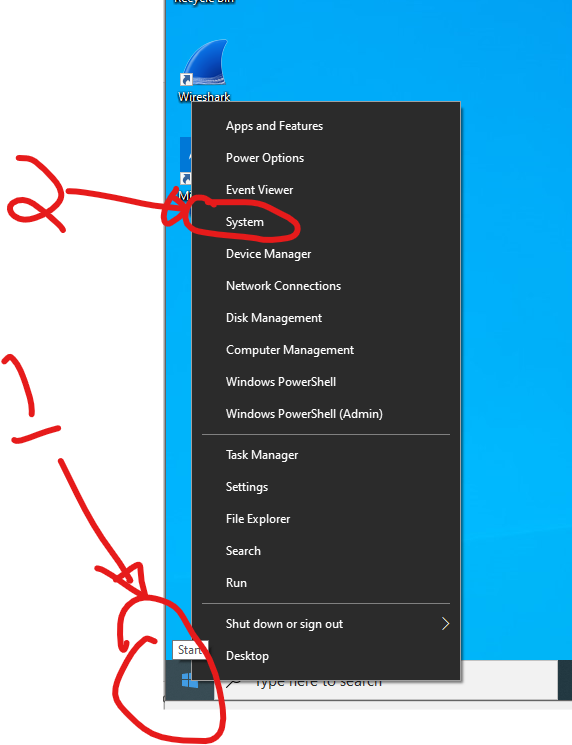
1. Take a screen of the Network Connection Details as a proof that you have completed the above exercise.

MINE BELOW

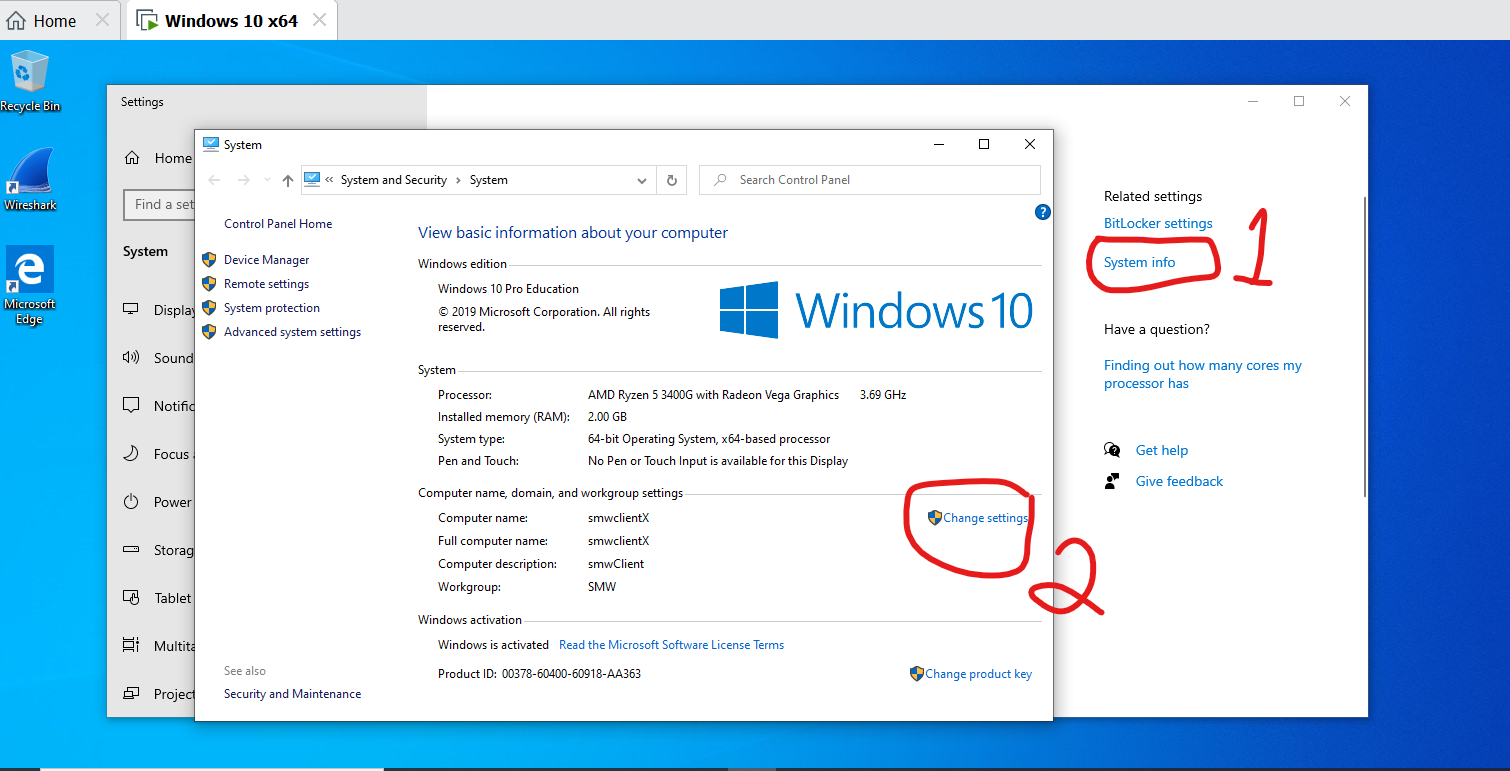
Graphical user interface, application

Description automatically generated

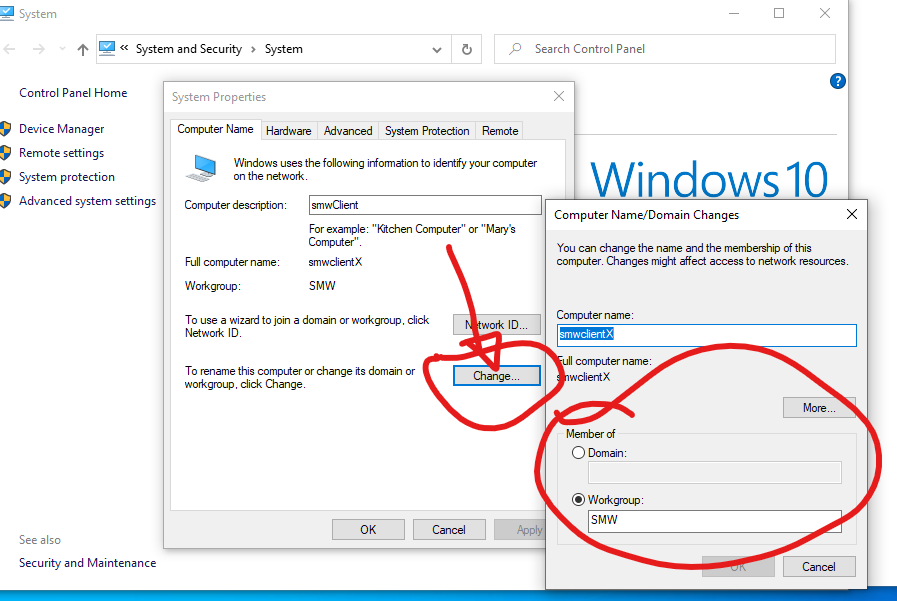
1. Close the Network Connections and its popups. Right-click on Windows Menu and select 'System'.



1. At the system settings page click on 'System info' to bring up the System Info Popup. Then click on the Change Settings link to bring up the system properties popup.



1. Click on the Change button to bring up the Computer Name/Domain Changes popup.



1. Update your computer name (e.g. client1). Select Domain. Enter your domain name, e.g. smw.soc.com. Click OK
2. You will be prompted to enter the Administrator and password for your Windows Server 2016 in order to join the domain. You may provide the smw\_srv2016 credential to proceed.
3. Your windows 10 will be restarted at this point to complete the join domain operation.

**Lab exercise 1-6 Logging onto Windows 10 with local and domain administrator**

1. Login to Windows 10 with the local administrator account by using “.\ladmin” as the username. A local user account exists only for that system locally. You cannot login with this account on to your Windows Server 2016.
2. Login to Windows 10 with the domain administrator account by using “smw\_srv2016@<your domain name>” (e.g. st2612@cat.cute.org) as the username. A domain account exists on all computers in the domain. You can use the domain Administrator account to login to both Windows 10 and Windows Server 2016 as they are both in the domain.

Reflection Prompts:

What is the main advantage to allow a user account to login to all the computers in the domain?

The advantage of using a domain user account is that the service's actions are limited by the access rights and privileges associated with the account. Unlike a LocalSystem service, bugs in a user-account service can't damage the system.

If the service is compromised by a security attack, then the damage is isolated to the operations that the system allows the user account to perform. At the same time, clients running at varying privilege levels can connect to the service, which enables the service to impersonate a client to perform sensitive operations.

[**https://learn.microsoft.com/en-us/windows/win32/ad/domain-user-accounts**](https://learn.microsoft.com/en-us/windows/win32/ad/domain-user-accounts)

**Optional Exploratory Exercises**

1. Explore what makes all the domain accounts can be logged on to the Windows 10 VM.
2. Search for a way to let your domain workstation (the Windows 10 Client) quit from the domain, ie. disjoin itself from the Domain.
3. Search and verify if there is a way to join domain only at the command prompt level (not using the GUI interface).

~ End of Practical 1~