**NSSA 221 Systems Administration I**

**Lab 02: Active Directory and Group Policy**

# **Introduction**

Active Directory allows Windows administrators to manage enterprise-wide information from a central repository in a distributed computer network. This lab will introduce you to the essential features that Active Directory offers and how they can be used to help manage user accounts, devices, and authentication. Throughout the lab, you will be introduced to various Active Directory terms such as objects, domains, organizational units, users, and groups. Active Directory is designed to align closely with a companies’ organizational structure. And while the lab covers these concepts on a much smaller scale, it should give you a sense of how Active Directory is implemented in a large organization. After the lab, you will have a basic understanding of the fundamentals that every system administrator must know to manage an Active Directory environment competently.

# **Lab Summary**

In this lab, you will install Active Directory, DNS, and DHCP on Windows Server 2022, and integrate these services into your virtual environment. Throughout the lab, you will perform various Active Directory administrative tasks to manage the environment remotely and locally. In addition to managing the server, you will create and enforce Group Policy Objects, or GPOs.

# **Goals**

At the end of this lab you will…

* Install and configure Active Directory, DNS, and DHCP on Windows Server 2022.
* Gain experience using Microsoft Windows Active Directory.
* Configure Group Policy Objects.
* Become familiar with Active Directory terminology.
* Develop a better understanding of how Active Directory aligns to an organization's structure.
* Manage user accounts in Active Directory using PowerShell and Active Directory Users and Computers, or ADUC.

# **Preparation**

* Optionally, read Chapters 4 and 5 from Windows Server 2022 Inside Out.
* Review Active Directory presentation

# **Activity Summary**

**Activity 1** – Install and Configure Windows Services

**Activity 2** – Create a Test User Account

**Activity 3** – Join the Test User to the Windows Domain

**Activity 4** – Remote Active Directory Management

**Activity 5** – Creating Organizational Units and Add Users

**Activity 6** – Creating and Implementing Group Polices

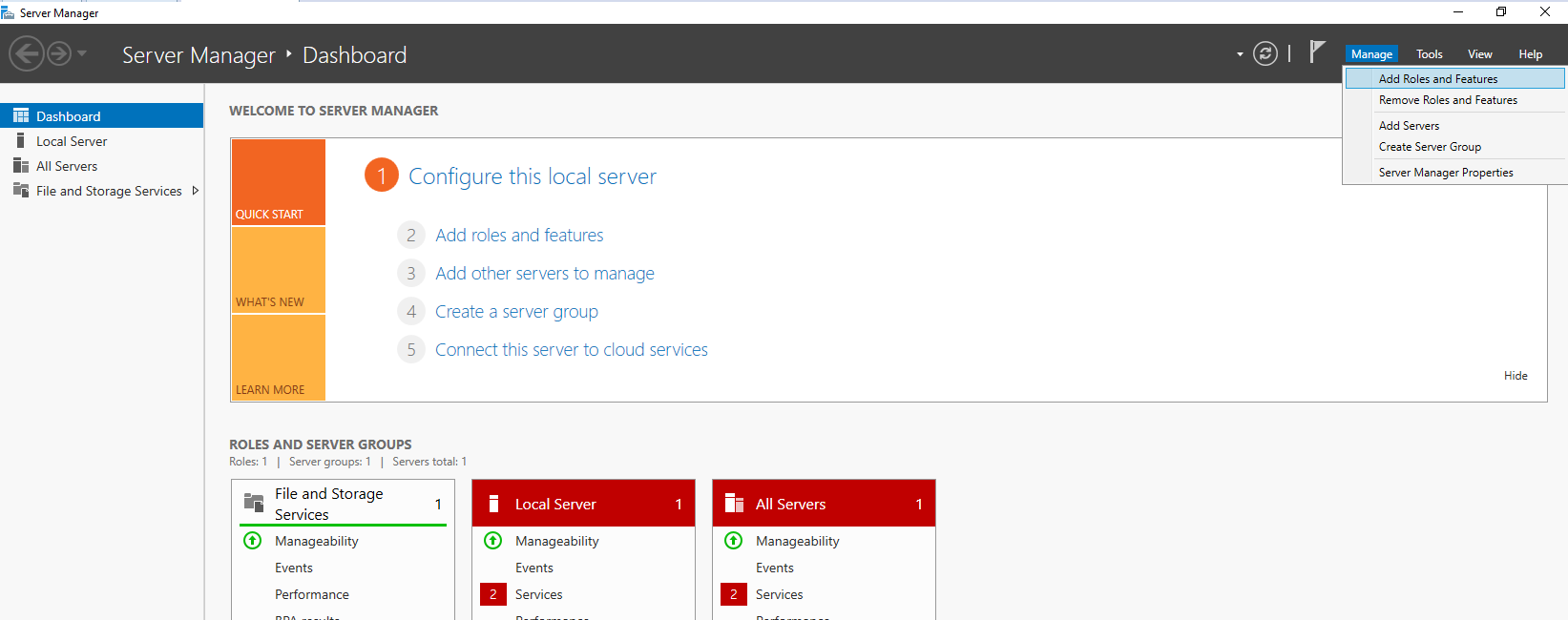
# **Activities**

## **Activity 1** – Install and Configure Windows Services

For this activity, you will be installing Active Directory Domain Services (AD DS), the Domain Name Service (DNS), and the Dynamic Host Configuration Protocol (DHCP) on Windows 2022 Server. Once the services are installed, you will then perform basic configuration for those services, join the clients to the domain, and remotely access the server using the RSAT utility and PowerShell.

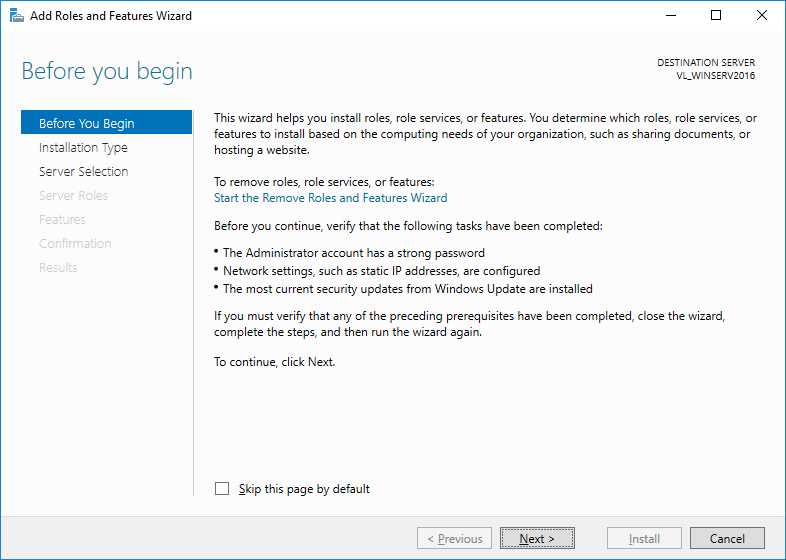
1. From *Server Manager 🡪 Dashboard,* select Manage and then “*Add Roles and Features*” to launch the wizard (Figure 1).

**Figure 1** – Add Roles and Features



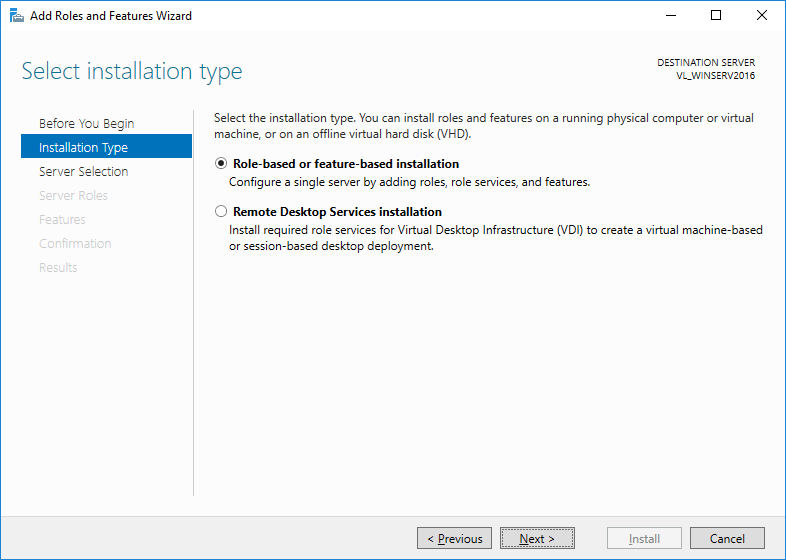
1. The first window will ask you to verify that certain tasks have been completed before you begin the installation (Figure 2). Read it and click, ***Next***.

**Figure 2** – Before you Begin



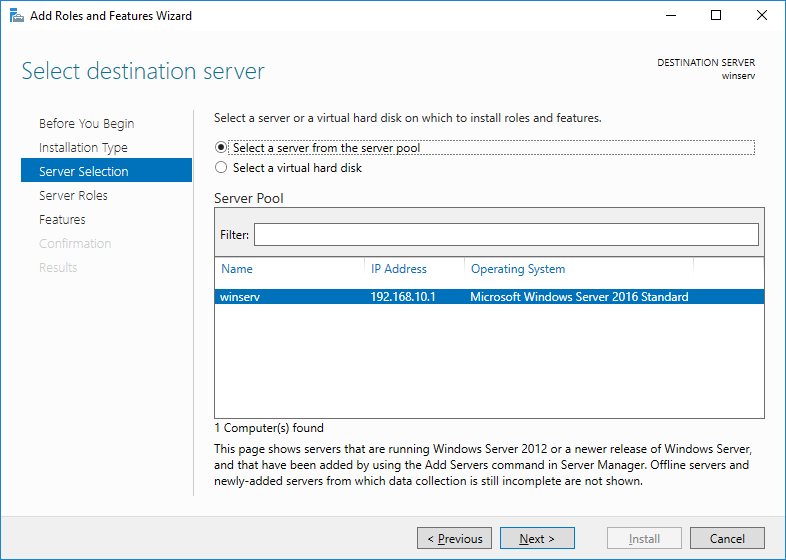
1. The next screen (Figure 9), will prompt you for the installation type, select “*Role-based or feature-based installation*,” and click ***Next***.

**Figure 3** – Select Installation Type



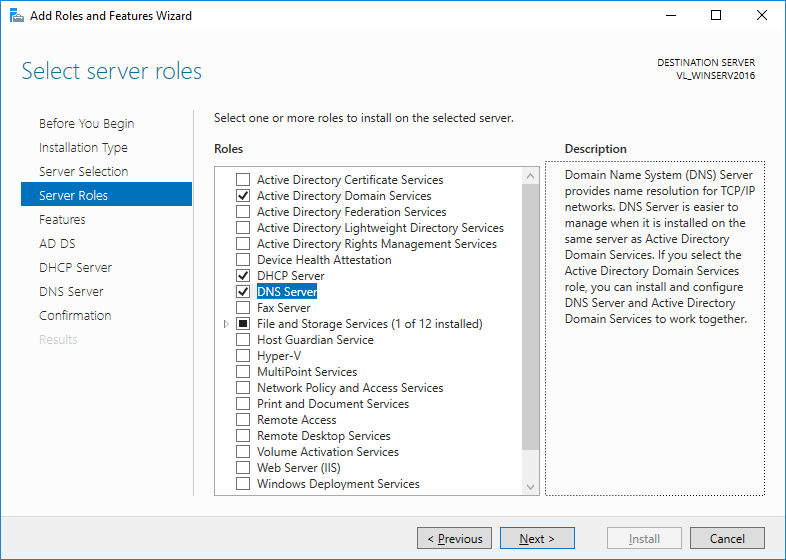
1. The next screen (Figure 4) will ask you to select the server, since this is the only server you currently have it will be selected by default, click ***Next***.

**Figure 4** – Select Destination Server



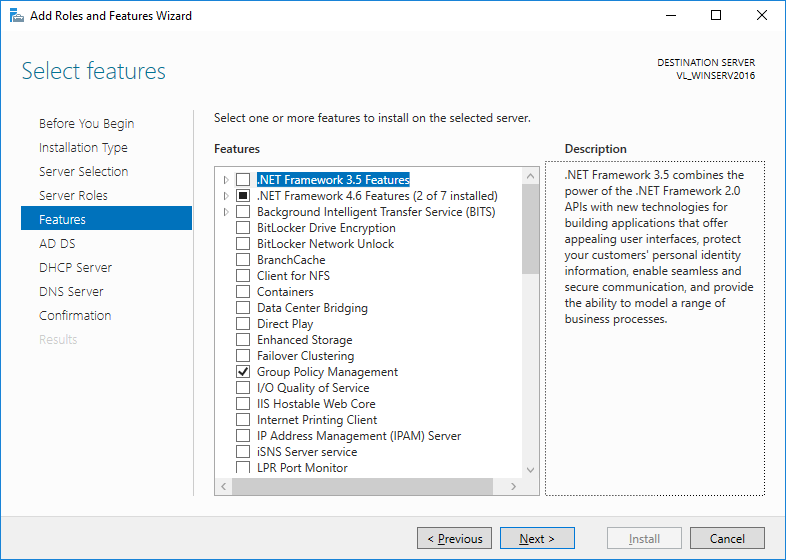
1. The next window (Figure 5) is where you select the three services, *Active Directory Domain Services*, *DHCP Server*, and *DNS Server*. For each service you will be prompted to Add Features, select the default features for each service. Once, all three roles have been selected hit ***Next***.

**Figure 5** – Select Server Roles



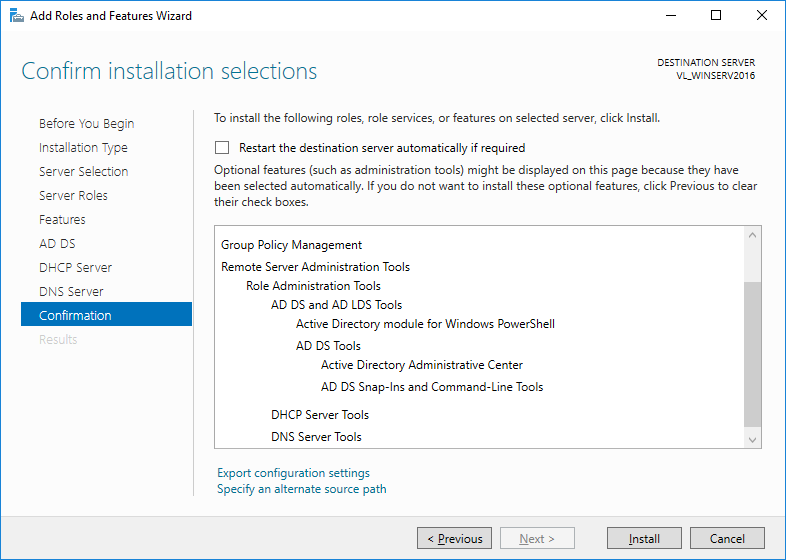
1. The next window gives you the option to select additional features (Figure 6), for our purposes we can use the default, “*Group Policy Management*.” Click, ***Next***.

**Figure 6** – Select Features



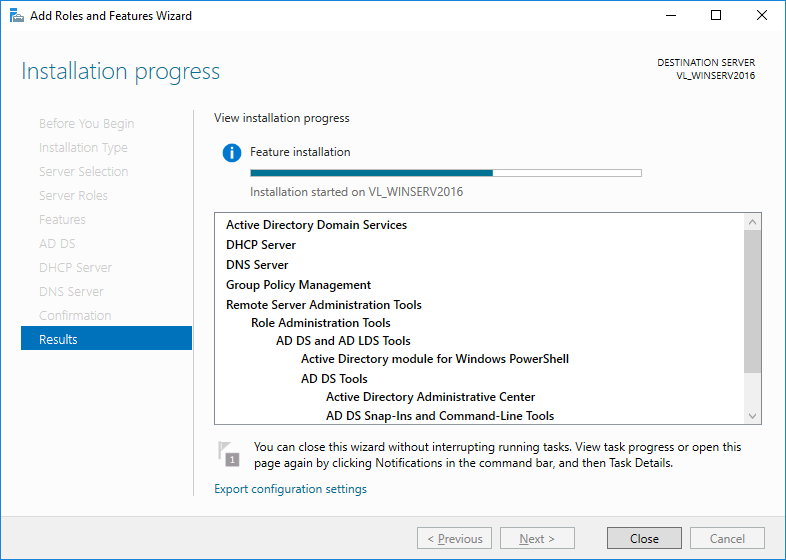
1. The next three windows will provide information about the services being installed, you can read the information or click ***Next***.
2. The second to last window asks you to confirm the installation selections (Figure 7). You do not need to check the box to restart the server, this is not required for the installation, but a restart will need to be done after the services are configured.

**Figure 7** – Confirm Installation Selections

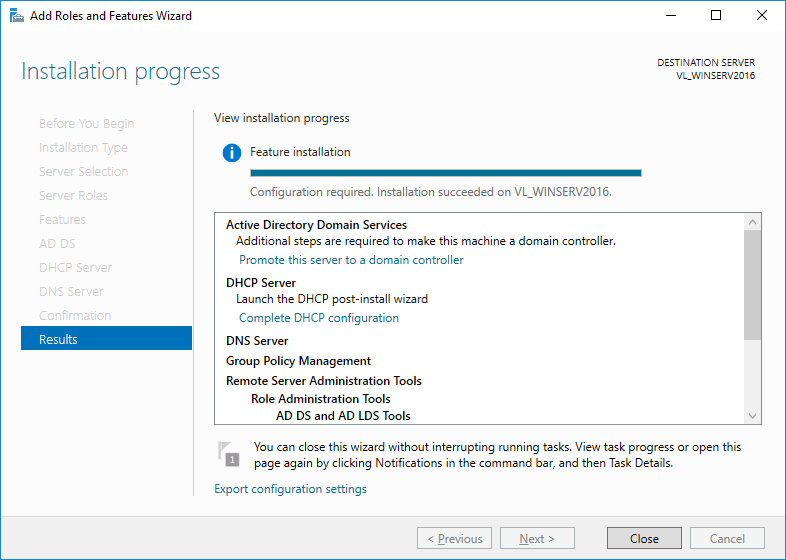


1. Click, ***Install***. Be patient, while the installation progresses (Figures 8 and 9).

**Figure 8** – Installation Progress

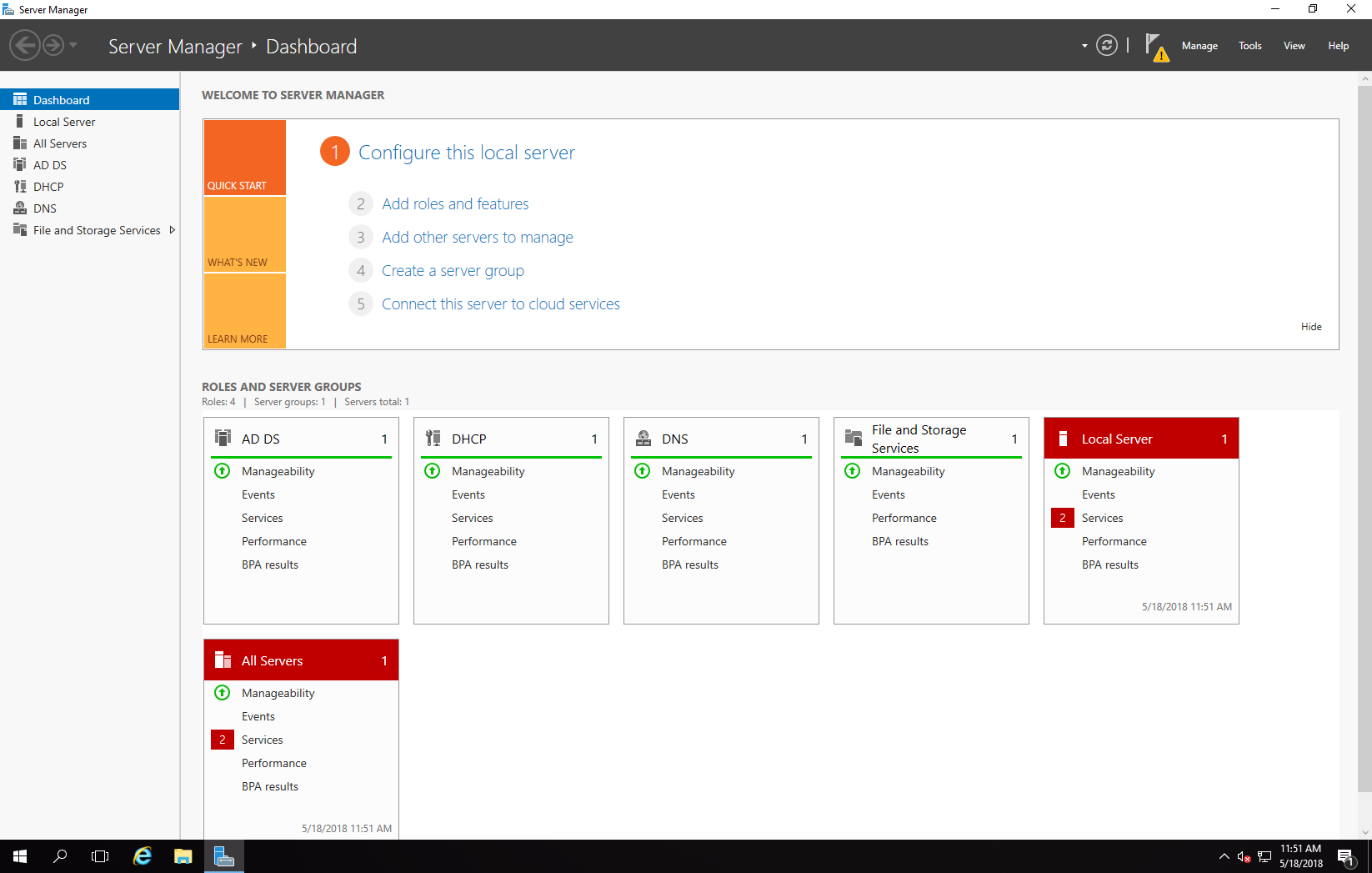


**Figure 9** – Installation Progress (cont.)



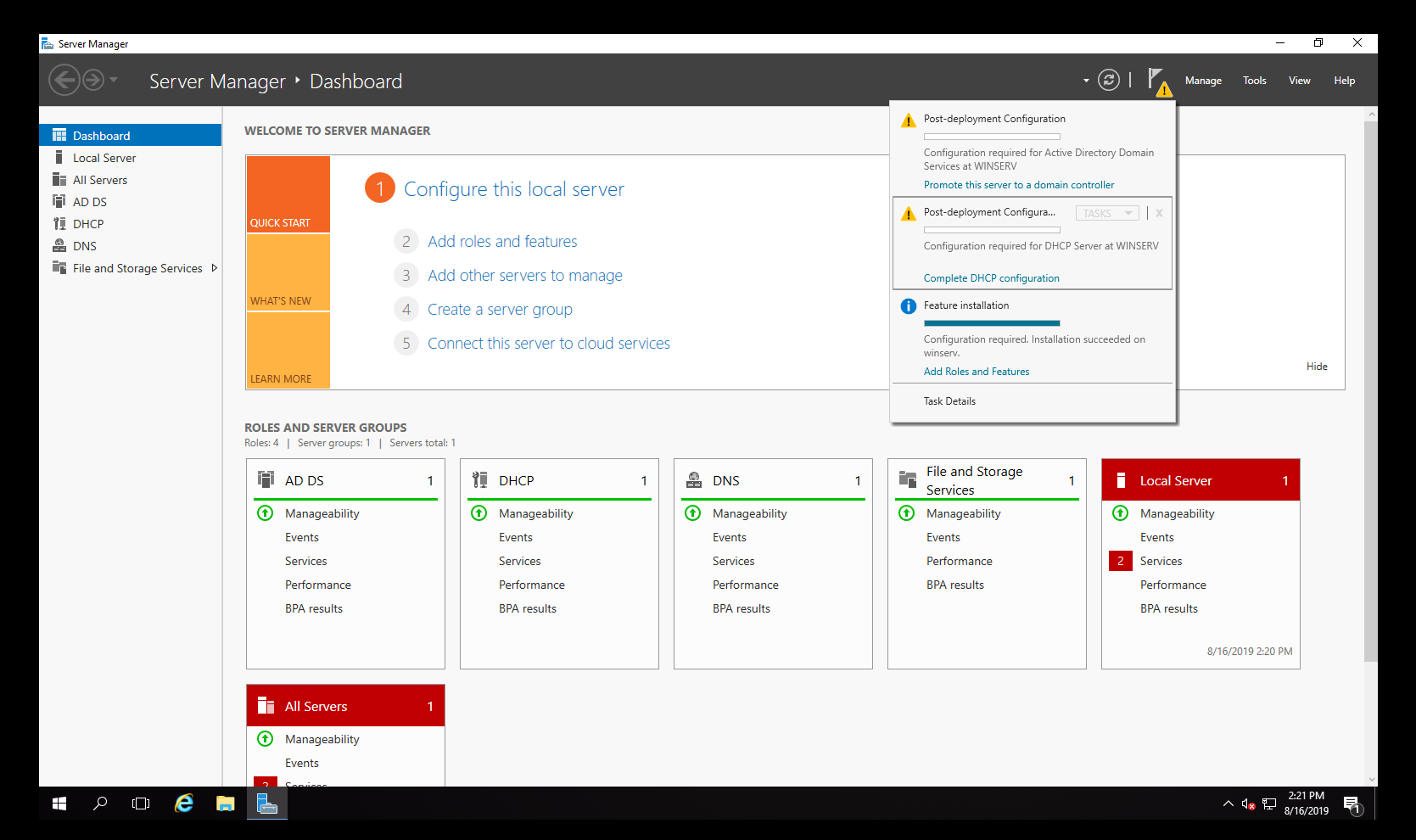
1. When the installation is complete you will see the new services available in the *Server Manager 🡪 Dashboard* (Figure 10).

**Figure 10** – Post Install Server Manager Dashboard



1. Notice the caution symbol next to the flag icon (Figure 11), click it, to bring up the notifications menu and click the link to “***Promote this server to a domain controller***” this will launch the Active Directory Services Configuration Wizard.

**Figure 11** – Post-Deployment Configuration





\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

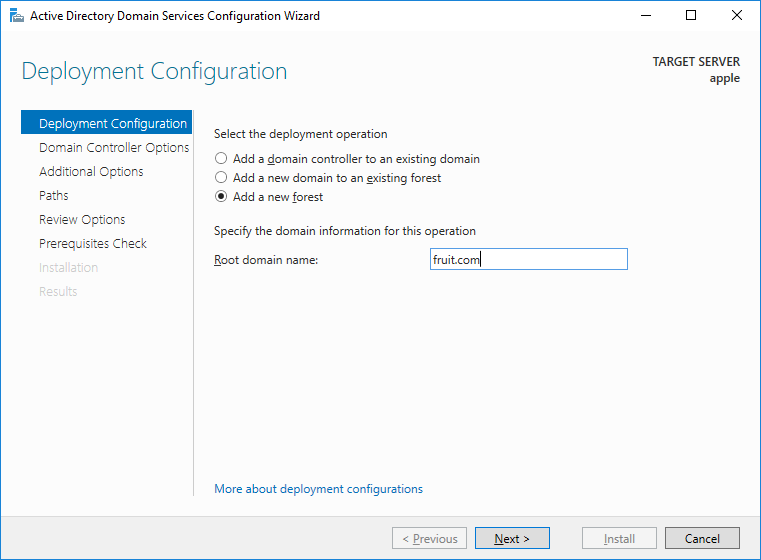
**Please Read! Please Read! Please Read! Please Read! Please Read!**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Your domain must be your **RIT Student ID**, followed by “.com”. If you **do not** name the domain your RIT student ID, you will receive a zero for the lab!

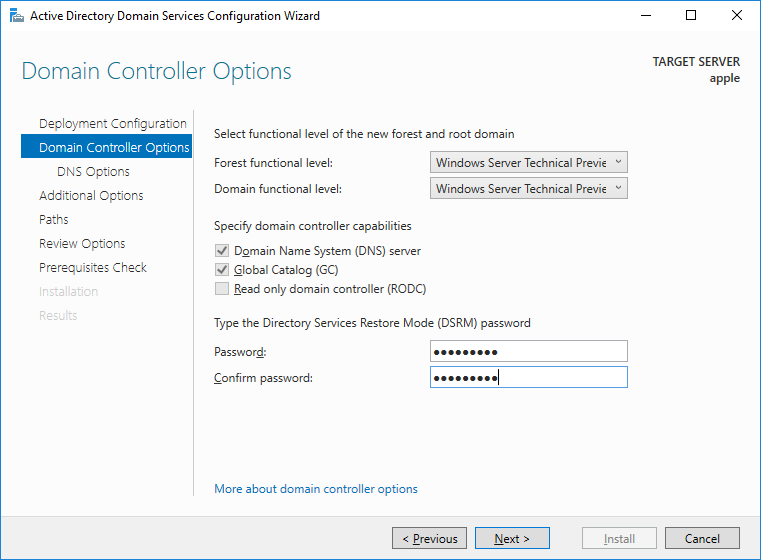
1. Select the “*Add a new forest*” radio button and enter your forest, i.e., your organizations’ domain (Figure 12). Your forest must be your student ID followed by “.com.” For example, *abc1234.com*. Click, ***Next***. **Do not use the example in these instructions.**

**Figure 12** – Add a New Forest



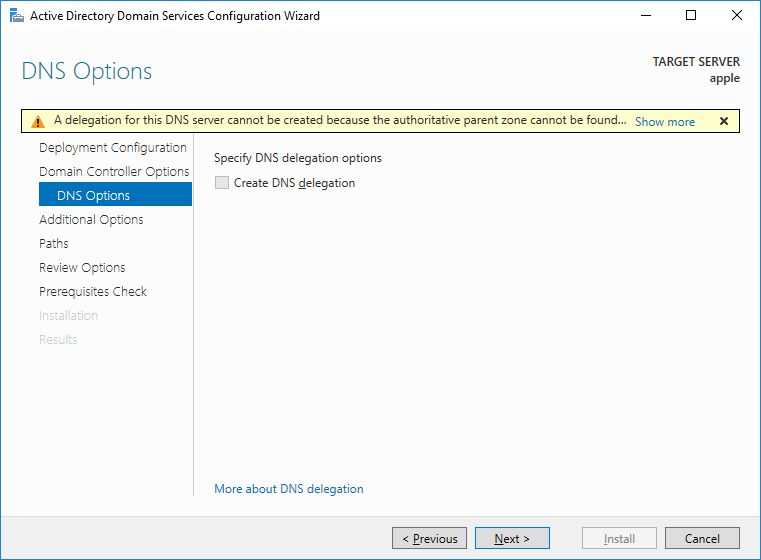
1. On the next screen (Figure 13) enter the password for the Directory Services Restore Mode (DSRM), chances are you will not be needing this but you may want to record the password nonetheless. Click, ***Next***.

**Figure 13** – Domain Controller Options



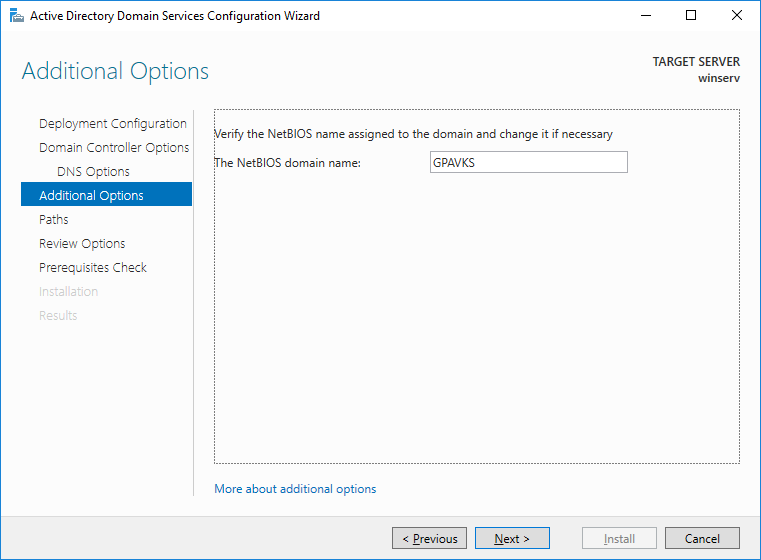
1. On the next screen (Figure 14), you are asked to create a delegation, since we are not registering the domain with a registrar, there is nothing to delegate, ignore the caution and click ***Next***.

**Figure 14** – DNS Options



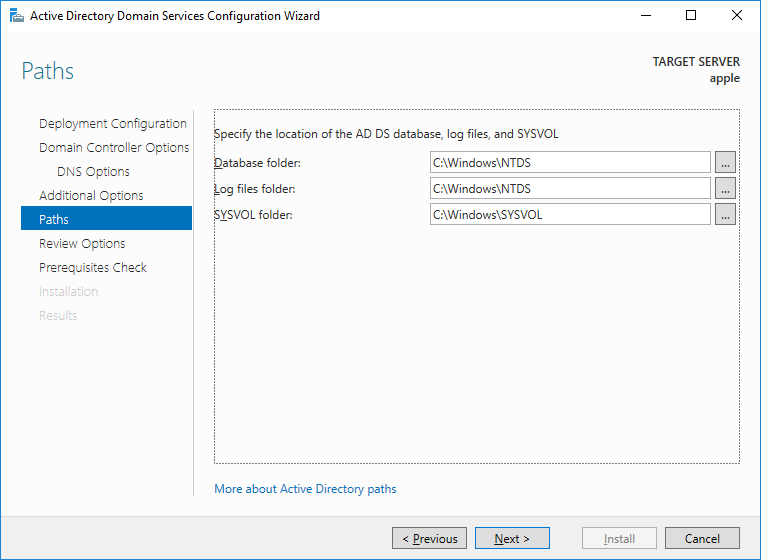
1. The next screen (Figure 15) will ask for the NetBIOS domain name, wait a moment for it to auto populate and click ***Next***.

**Figure 15** – Additional Options



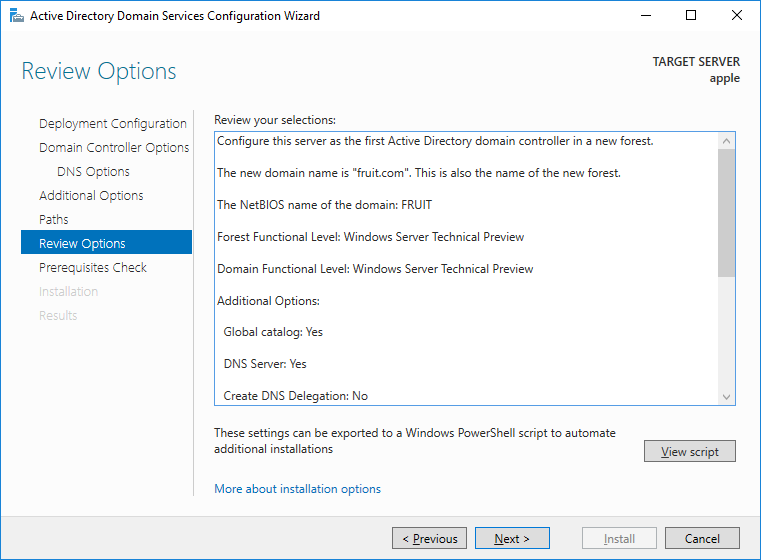
1. The next screen (Figure 16) will ask where you want to locate the AD DS database, log files, and SYSVOL, use the defaults and click ***Next***.

**Figure 16** - Paths



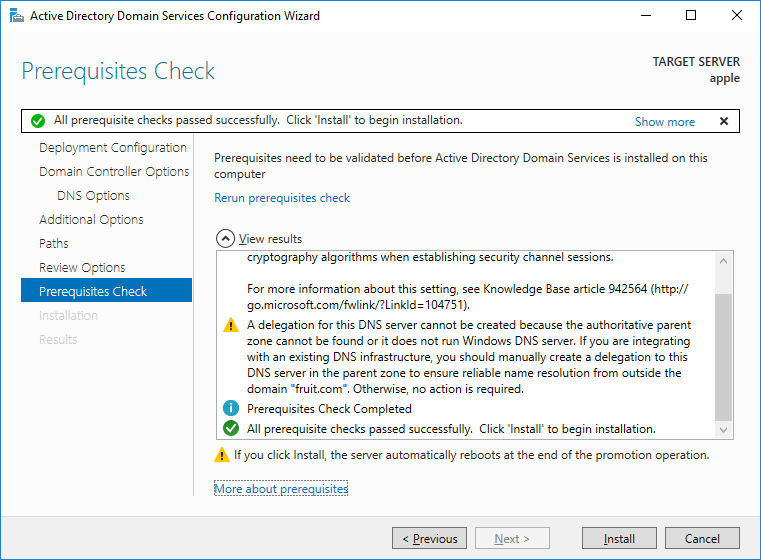
1. The next screen (Figure 17), gives you the opportunity to review your configuration settings. You can also export a PowerShell script to automate future installations. Click, “*View script*” and **save the file**, you will need it for the next lab. Click, ***Next***.

**Figure 17** – Review Options



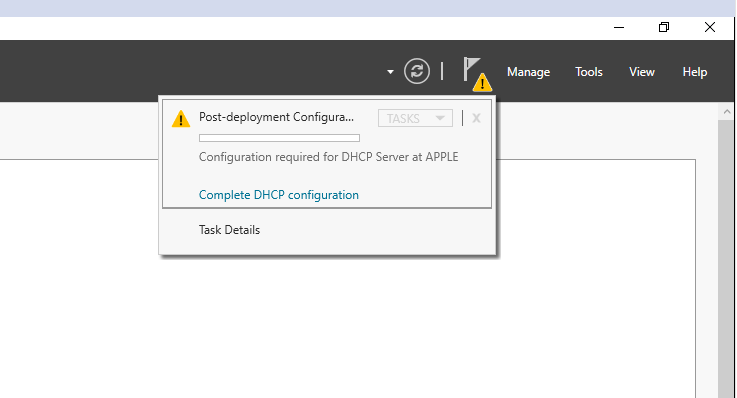
1. Finally, Windows will perform a prerequisite check (Figure 18), once the checks have passed and you see the green check symbol, click the *Install* button.

**Figure 18** – Prerequisite Check



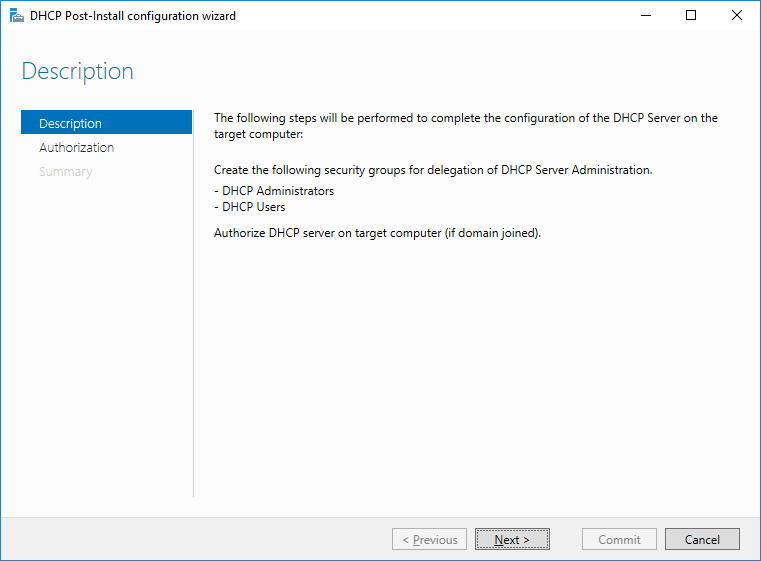
1. The installation will take several minutes to complete, **be patient!** When you reboot the server you may need to change the Administrator password.
2. Next, you will need to configure the DHCP settings. Click the notifications flag (Figure 19) and select “*Complete DHCP configuration*” to launch the DCHP Post-Install configuration wizard. This will configure who has the ability to manage the DHCP server.

**Figure 19** – DHCP Configuration



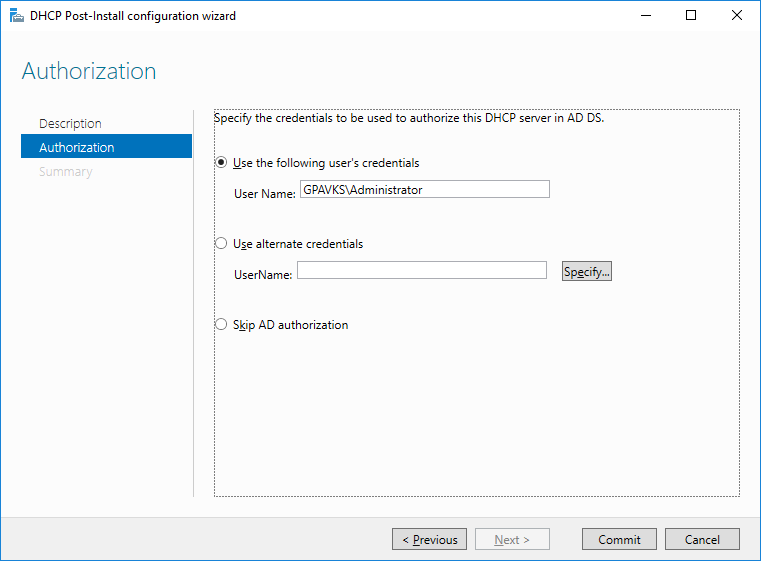
1. The first window to appear will give you information about what you are configuring (Figure 20), read it and click ***Next***.

**Figure 20** – DHCP Post-Install Configuration Wizard



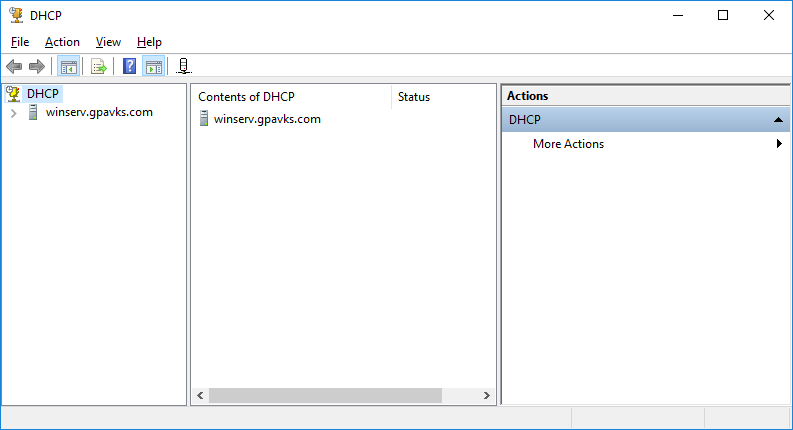
1. The next screen (Figure 21) allows you to select who will be authorized to make changes to the DHCP server, for this lab the Administrator account will be used. Click the ***Commit*** button and then the ***Close*** button on the *Summary* window.

**Figure 21** – Authorization



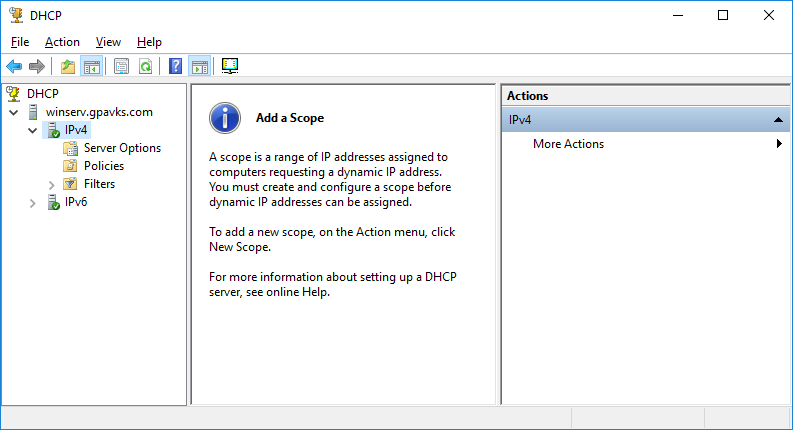
1. To configure the default IP addresses, gateway, and DNS server perform the following steps. From *Server Manager 🡪 Dashboard*, select ***Tools***. From the dropdown menu click ***DHCP***.

**Figure 22** – DHCP



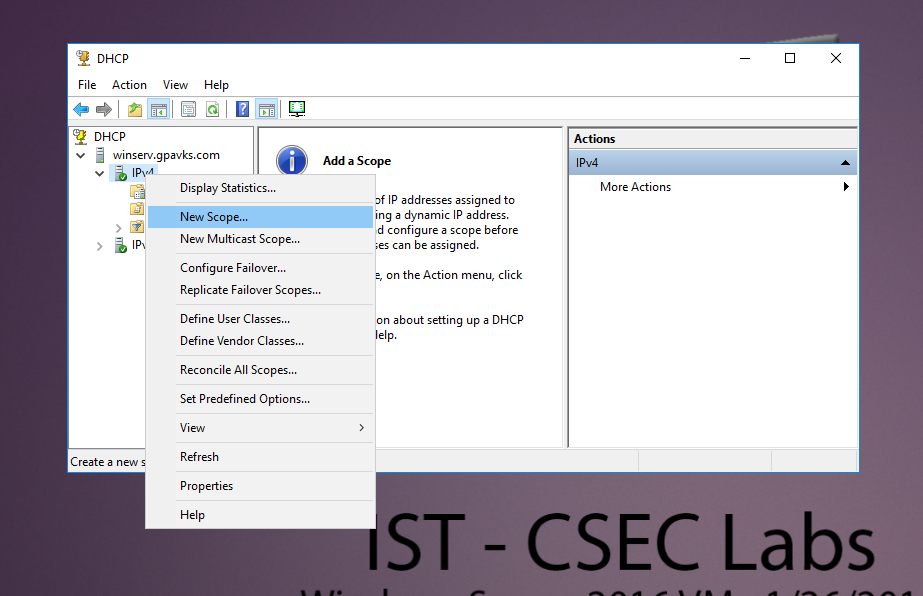
1. From the DHCP configuration window (Figure 28) expand the menu for the server to reveal IPv4 (Figure 23).

**Figure 23** – Add Scope

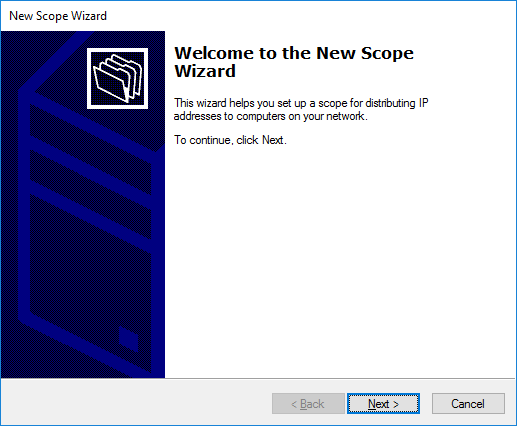


1. Right click on IPv4 and select ***New Scope*** from the dropdown menu (Figure 24). This will launch the New Scope Wizard (Figure 25). Click, ***Next***.

**Figure 24** – New Scope

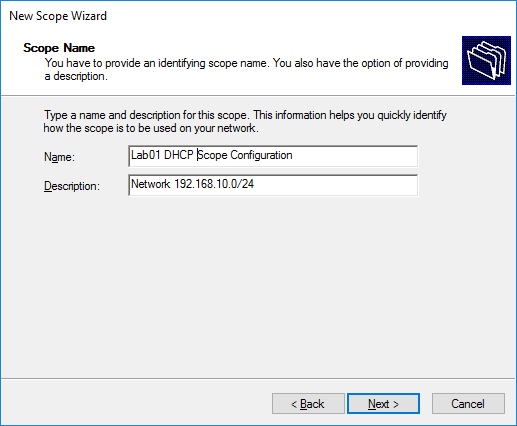


**Figure 25** – New Scope Wizard



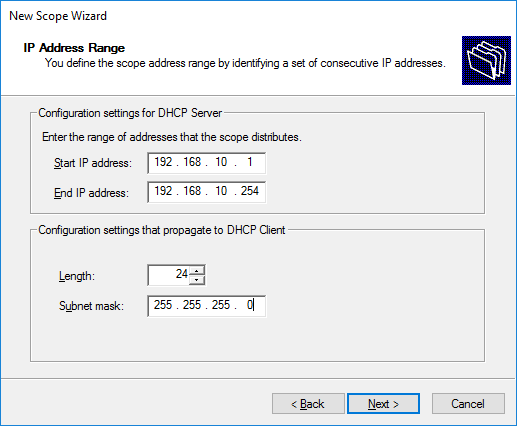
1. On the next window (Figure 26) you may enter a name and description. Click, ***Next***.

**Figure 26** – Scope Name/Description



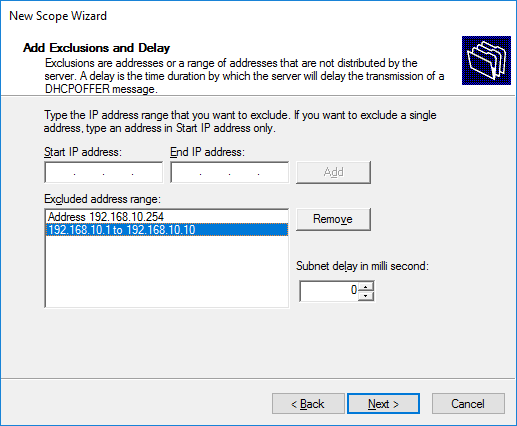
1. Next, define the range of IP addresses that will be available to pass out to clients (Figure 27). Be sure to include the network mask and click ***Next***. Again, based on what you did in *Introduction to Routing and Switching* you should have a fundamental understanding of IP addressing and masks.

**Figure 27** – IP Address Range



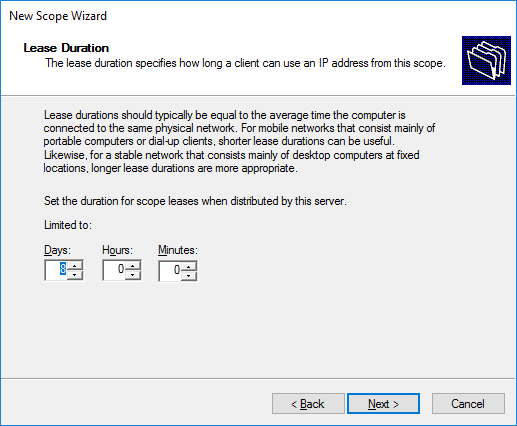
1. On the next window, configure two exclusions, one for the gateway, and another for servers. Exclude the static IP assigned to the default gateway (the pfSense LAN interface). Then, set aside a range of addresses to be assigned to servers throughout the semester, five is sufficient. Referring to the range in Figure 28, addresses 192.168.10.1 through 192.168.10.10 and address 192.168.10.254 are excluded. Click, ***Next***.

**Figure 28** – IPv4 Address Exclusions



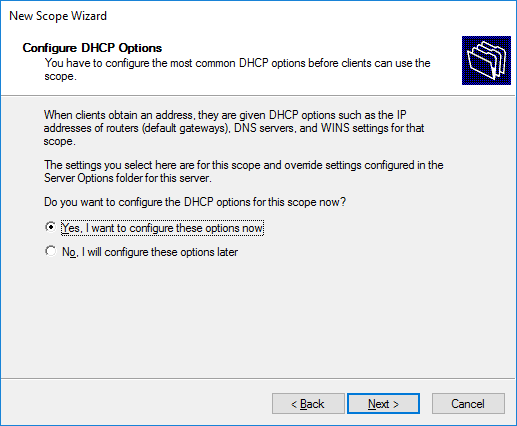
1. Since lab occurs once a week the default setting (8 Days) for the lease time is sufficient (Figure 29). Click, ***Next***.

**Figure 29** – Lease Times



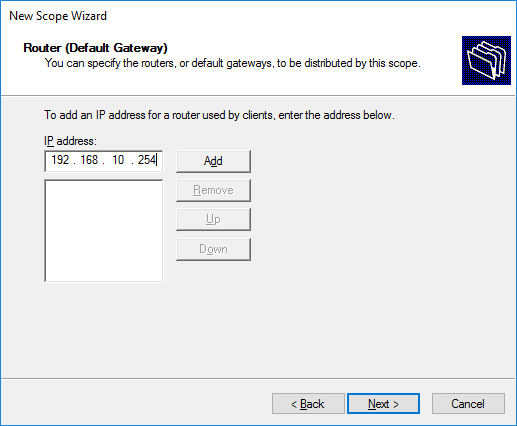
1. Next, configure the default gateway, and DNS servers by selecting “*Yes. I want to configure these options now*” (Figure 30) and click ***Next***.

**Figure 30** – Configure DHCP Options



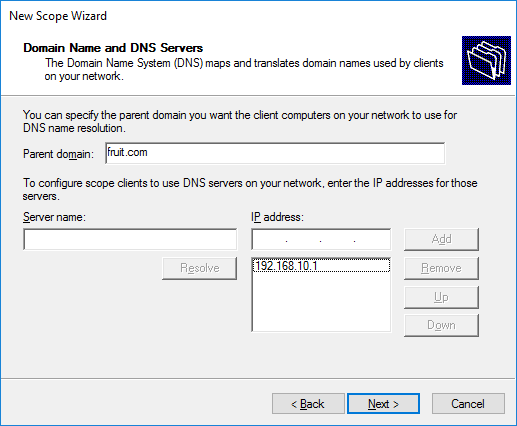
1. On the next window (Figure 31) enter the default gateway (the LAN interface for pfSense) for your network and click ***Add*** and then ***Next***.

**Figure 31** - Configure Default Gateway



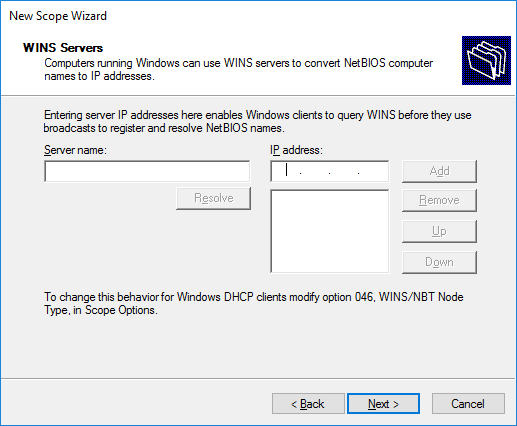
1. On the next screen (Figure 32), by default, the servers IP address will already be listed as the address for the DNS server, this is what we want. Click, ***Next***.

**Figure 32** – Domain Name and DNS Servers



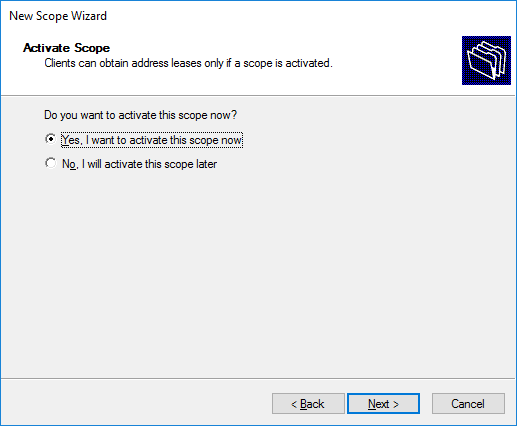
1. We do not need to configure anything for the Windows Internet Naming Servers, or WINS (Figure 33), click ***Next***. If you’re curious, the option is there for backward compatibility with legacy Windows environments.

**Figure 33** – WINS Servers



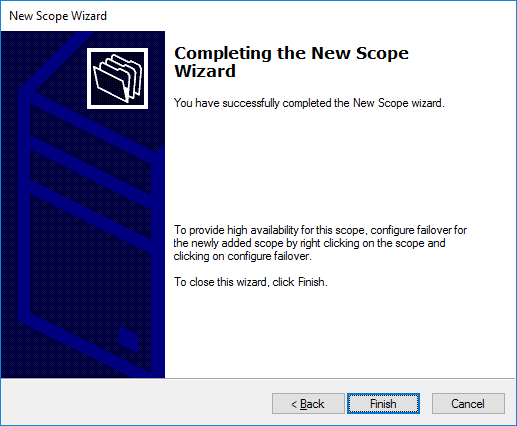
1. On the next window (Figure 34) activate the scope by selecting the “*Yes. I want to activate this scope now*,” radio button and clicking ***Next***.

**Figure 34** – Activate Scope



1. Complete the configuration by clicking ***Finish*** (Figure 35).

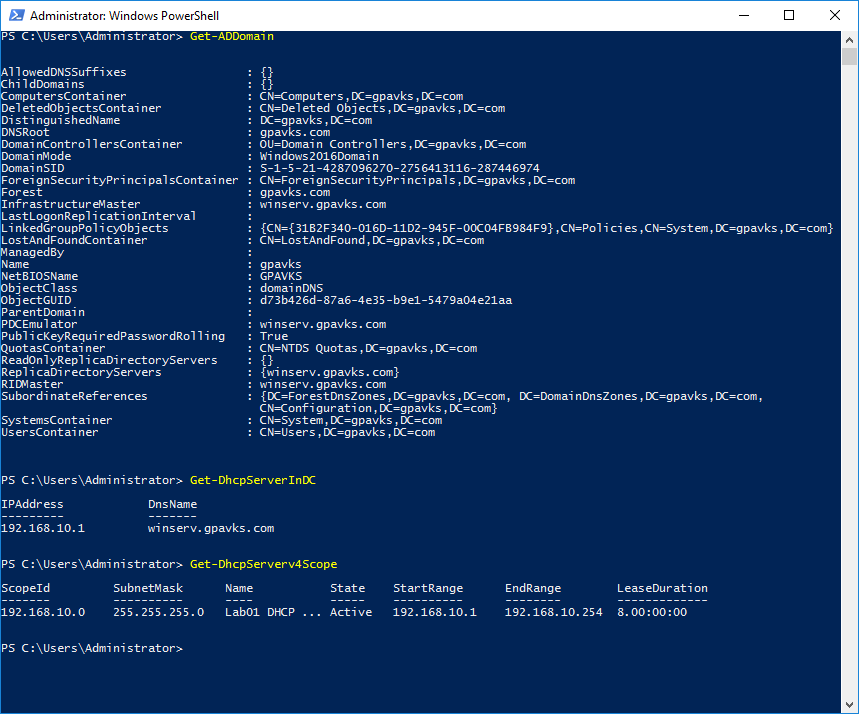
**Figure 35** – Completing the New Scope Wizard





In the report, include a **single** screenshot that shows the domain information, the DHCP server, and scope. Open PowerShell and log in as Administrator, use the following commands to display the required information, Get-ADDomain, Get-DhcpServerInDC, and Get-DhcpServerv4Scope. Figure 36, provides an example of the output. This must be a **single** screenshot and include **ALL** the required information to receive credit.

**Figure 36** – AD and DHCP Server Information Sample Screenshot

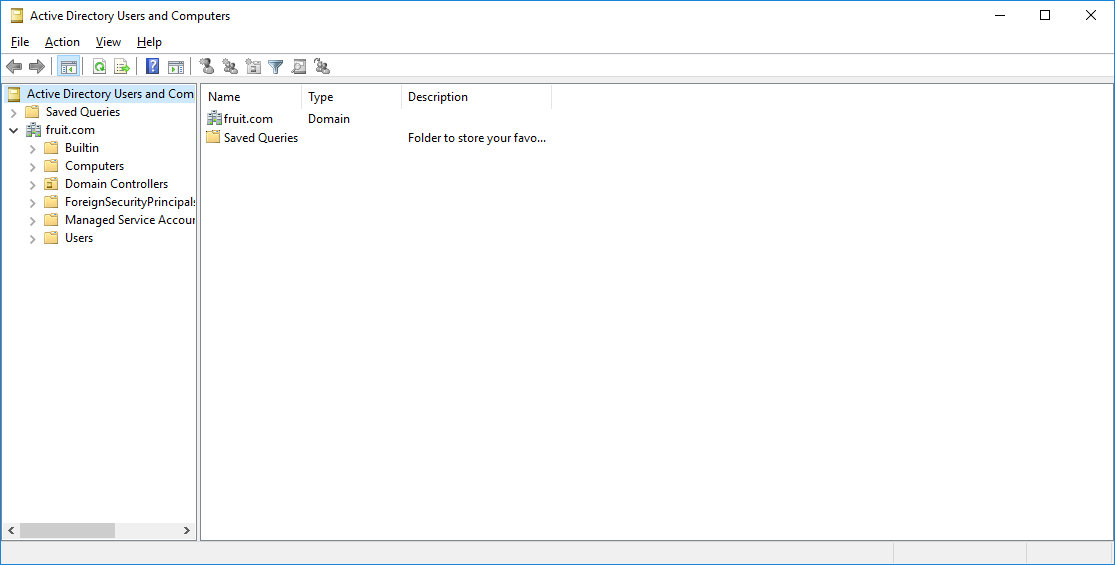


## **Activity 2 – Create a Test User Account**

Generally speaking, a Domain Controller controls who can access services in the domain and to establish administrative and security boundaries. Linux implementations may use FreeIPA or Samba/Winbind for a domain controller. But for this activity, you will be authenticating a user from both the Linux and Windows clients using the Windows Active Directory Service.

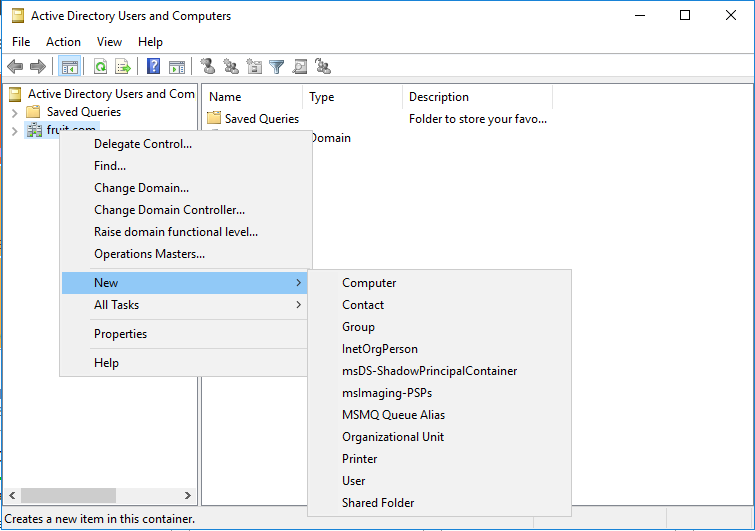
1. On Windows Server 2022, return to the *Server Manager 🡪 Dashboard* and select *Tools 🡪 Active Directory Users and Computers*. This will produce the following window (Figure 37).

**Figure 37** – Active Directory Users and Computers (ADUC)



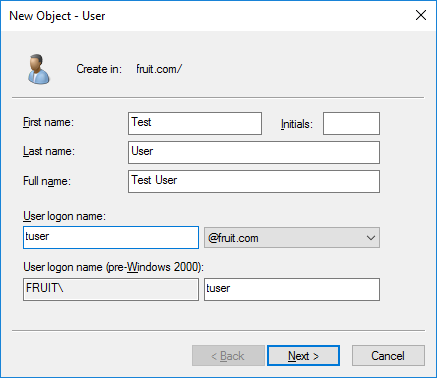
1. Right-click on the domain, from the dropdown menu select *New 🡪 User (Figure 38)*.

**Figure 38** – Create a New User



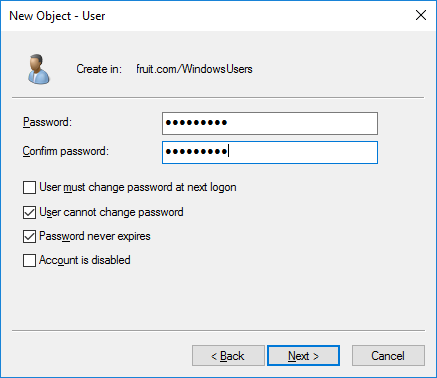
1. Create the *New Object – User*, and referring to Figure 39, enter the users first, last, and logon name.

**Figure 39** – New User Creation



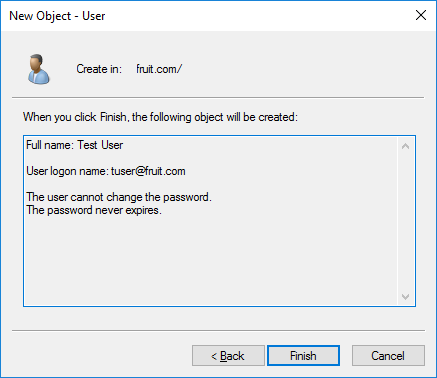
1. Enter a password for the newly created user and uncheck “*User must change password at next logon*”, check the boxes for “*User cannot change password*” and “*Password never expires*”, click ***Next*** (Figure 40).

**Figure 40** – Password Configuration

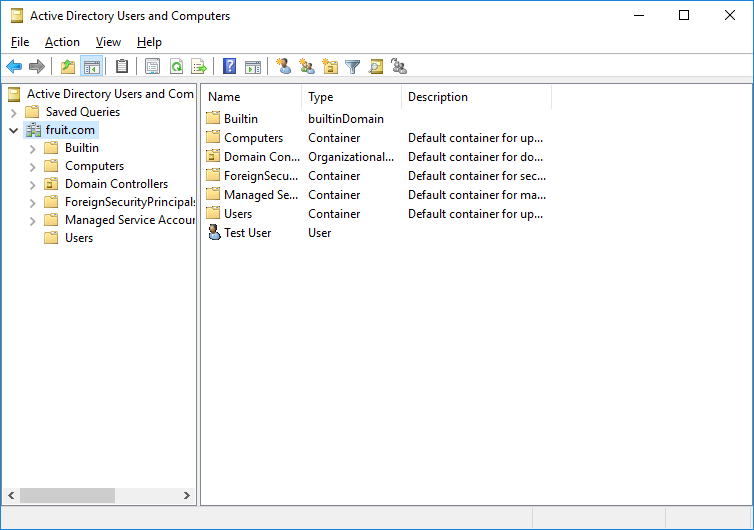


1. The next window, Figure 41, provides a summary of the user information, click ***Finish***.

**Figure 41** – User Creation Summary Window

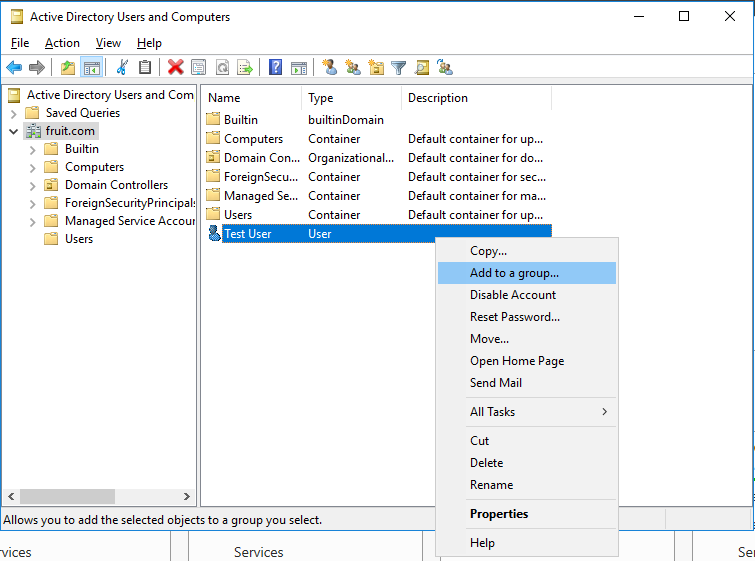


1. The user will appear in the domain (Figure 42).

**Figure 42** – Created User in the domain

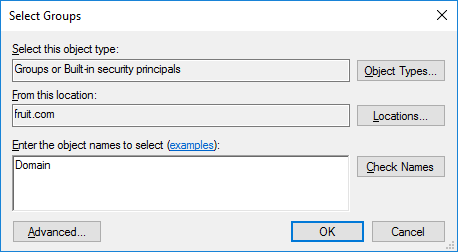
1. Next, we are going to add the user to the *Domain Admin* group, by right-clicking on the user and selecting “***Add to a group***” from the dropdown menu (Figure 43).

**Figure 43** – Add to a Group

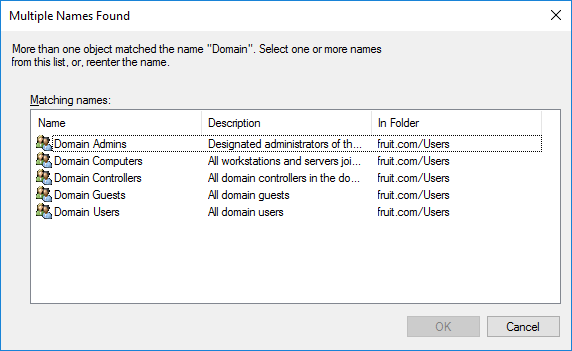


1. From the *Select Groups* window (Figure 44) search by entering “*Domain****”*** into the “*Enter the object names to select*” field. And then click the *Check Names* button, select *Domain Admins* (Figure 46) from the list of options, the field will populate with Domain Admins (Figure 45), click ***OK***.

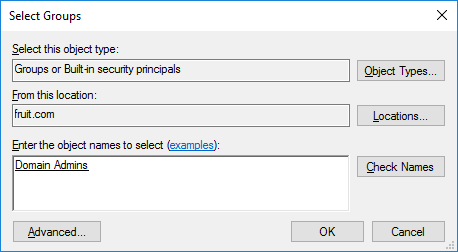
**Figure 44** – Select Groups



**Figure 45** – Matching Names

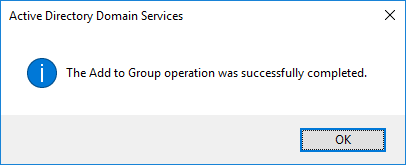


**Figure 46** – Select Group



1. The final window will confirm that the user was added to the group, Figure 47.

**Figure 47** – User Successfully Added Confirmation



## **Activity 3 –** Join the Test User to the Windows Domain

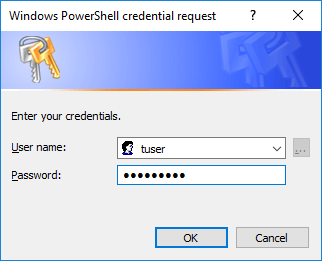
For this activity, you will join the Windows 10 and Linux client to the Windows domain using the test user you created in the previous activity.

1. Power on the Windows and Linux clients. Again, make sure to attach the virtual NICs to the LAN Segment.
2. Change the NIC settings on the clients to receive their respective IPv4 network configurations via DHCP.
3. On Windows 10, open PowerShell and run as Administrator.
4. Enter the following command, using your domain suffix.



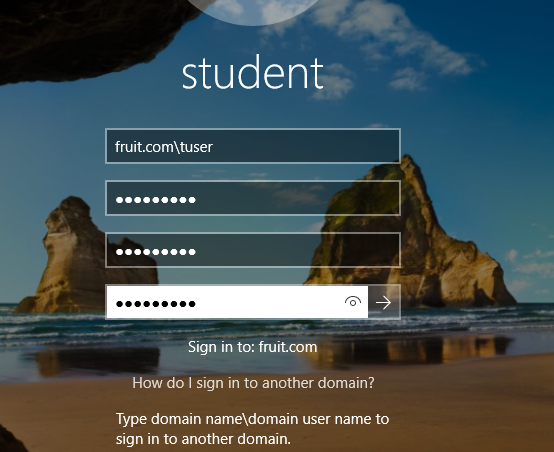
1. When prompted enter the test users’ user name and password, Figure 48.

**Figure 48** – Windows 10 Credential Request



1. Click OK and restart Windows 10.
2. After the restart you maybe prompted to change the user password. When you log into Windows 10 as a domain user you can use the canonical form, domain\user (Figure 49). Alternatively, you can use the User Principal Name, or UPN.

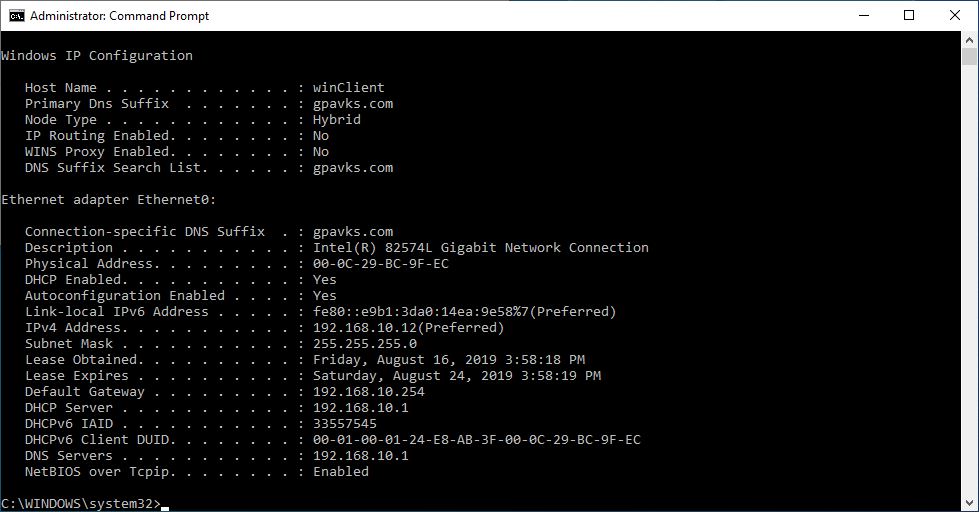
**Figure 49** – Logging into Windows 10





For the report, you will need **three** screenshots. One will show that Windows 10 received its IP address from the Windows server, and it must show **ALL** of the IP configuration **AND** adapter settings (Figure 50).

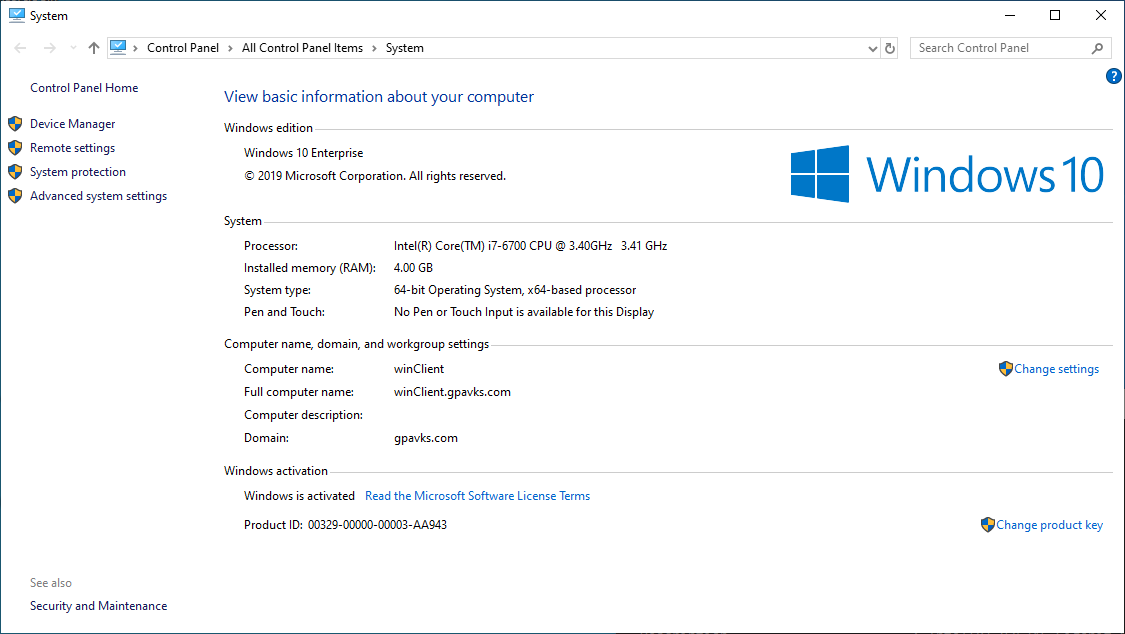
**Figure 50** – Sample Screenshot Showing Network Configuration Settings for Windows 10



The screenshot **must** show the following information to receive credit. If any of the information is missing or illegible you will not receive credit for the screenshot.

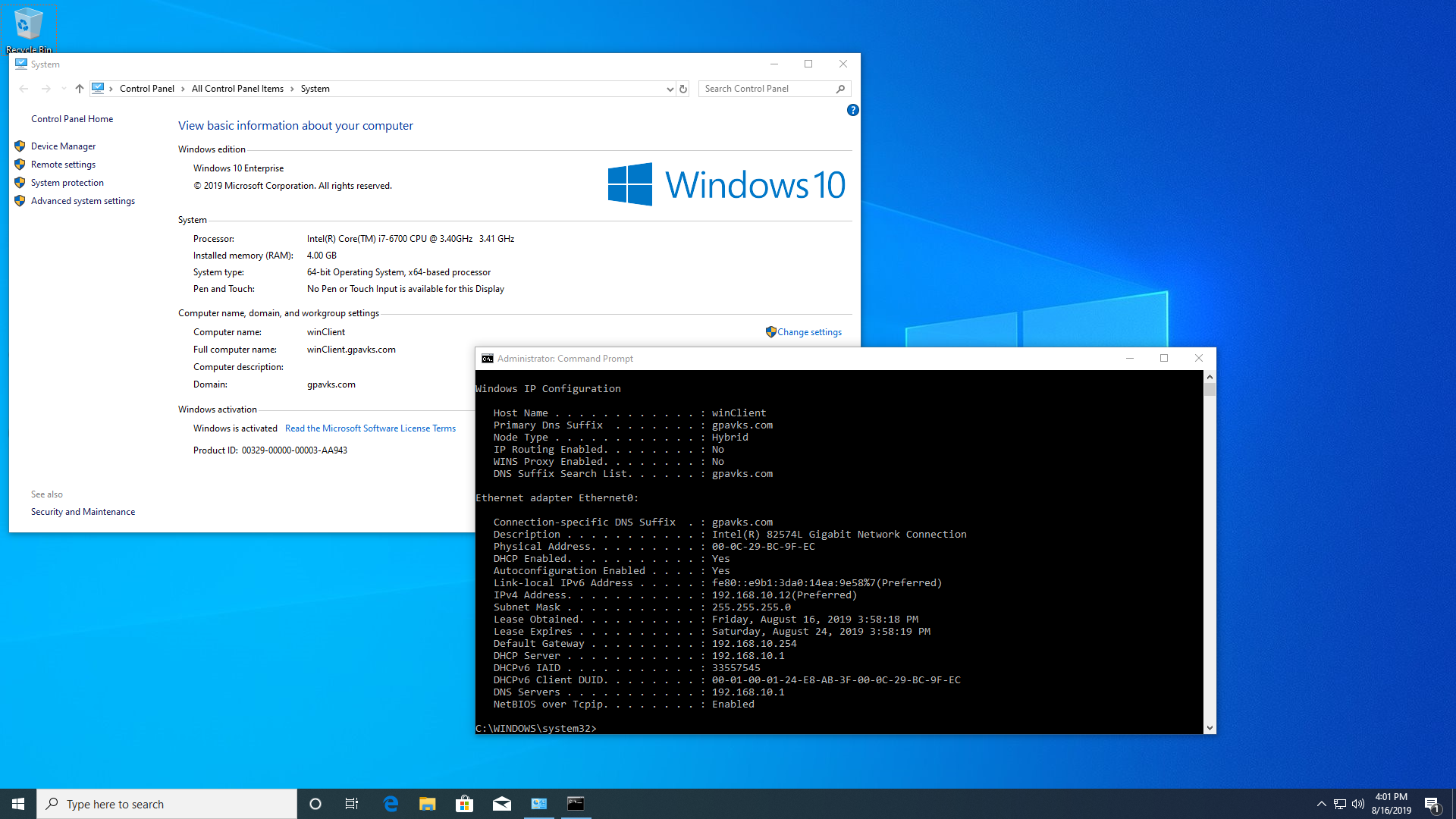
* The Host Name
* The Primary DNS Suffix
* DHCP enabled, Yes
* DHCP lease information
* The DHCP server
* The DNS server

The second screenshot, must show that the Windows client is a member of the domain (Figure 51).

**Figure 51** – Sample Screenshot Showing Windows 10 Domain Information

The third screenshot will show the previous two screenshots together. DO NOT cover up the domain information (Figure 52).

**Figure 52** – Domain and Network Configuration Verification

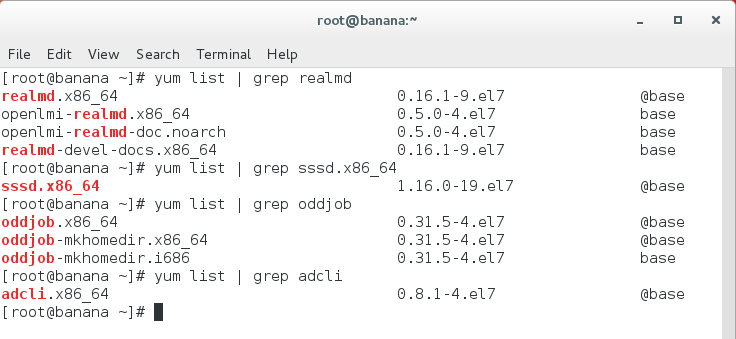
****

1. On the Linux client, log in as “*student*”, using the default password “*student*”. Optionally, for convenience, you may want to log in as “*root*”.
2. Open a terminal, go to Applications 🡪 System Tools 🡪 Terminal, and verify you can resolve ping requests to Googles’ public DNS by pinging 8.8.8.8, and that you can resolve DNS by pinging “google.com”.
3. Update the CentOS 7 VM by typing the following command.



1. The update may take some time, so be patient. Or nothing will need to be updated if you updated the system in Lab 00.
2. By default, the following packages are installed, but let’s check to be sure.
   * realmd
   * sssd
   * oddjob
   * oddjob-mkhomedir
   * adcli
3. Referring to Figure 53, using the **dnf list** command and by piping grep, we can check that the system has the required installed packages. Remember, the **dnf** command replaces **yum** in CentOS 8, although you can still use the **yum** command as it is backward compatible.
4. .

**Figure 53** – Checking SSSD is installed



1. If any packages are missing, use dnf to install them.
2. You may also want to check to verify that the realmd and sssd services are running. The following command checks the status of realmd.



1. If you need to start the service, type the following command.



1. To make sure the service starts when the system boots, use the following command. 
2. If you need more information on how to start, stop, and enable services, refer to the **man pages** for the systemctl command.
3. The following command will join the user to the Active Directory domain. Make sure to substitute your domain and user information with the example provided.

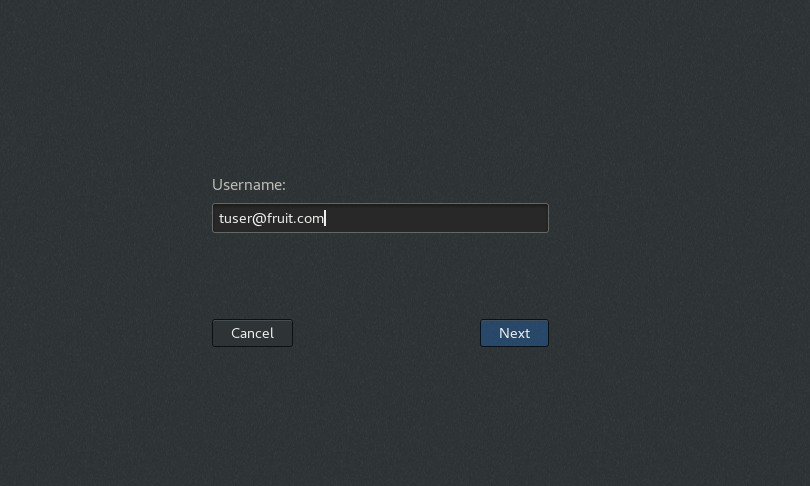


Or



1. To verify that the user can join the domain, log out as the current user, and log in as the Active Directory user. The example, in Figure 54 shows tuser, logging into the fruit.com domain using the User Principal name (UPN). CentOS needs the UPN.

**Figure 54** – CentOS 7 Log In

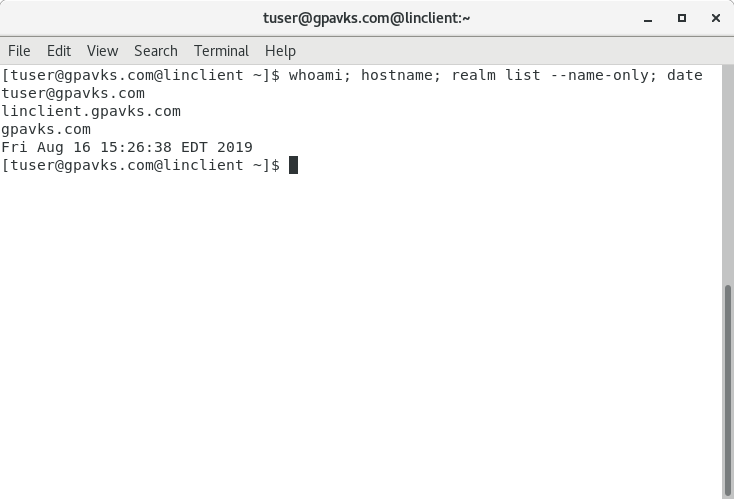




To validate that you have completed this activity, you must include a **single** screenshot in the lab report. The screenshot must include the following information, the date, the Active Directory user logged in, the realm and the host name. The following commands will provide this information. Figure 55 provides an example.

* date
* whoami
* hostname
* realm list –name-only

**Figure 55** – CentOS 7 Verification



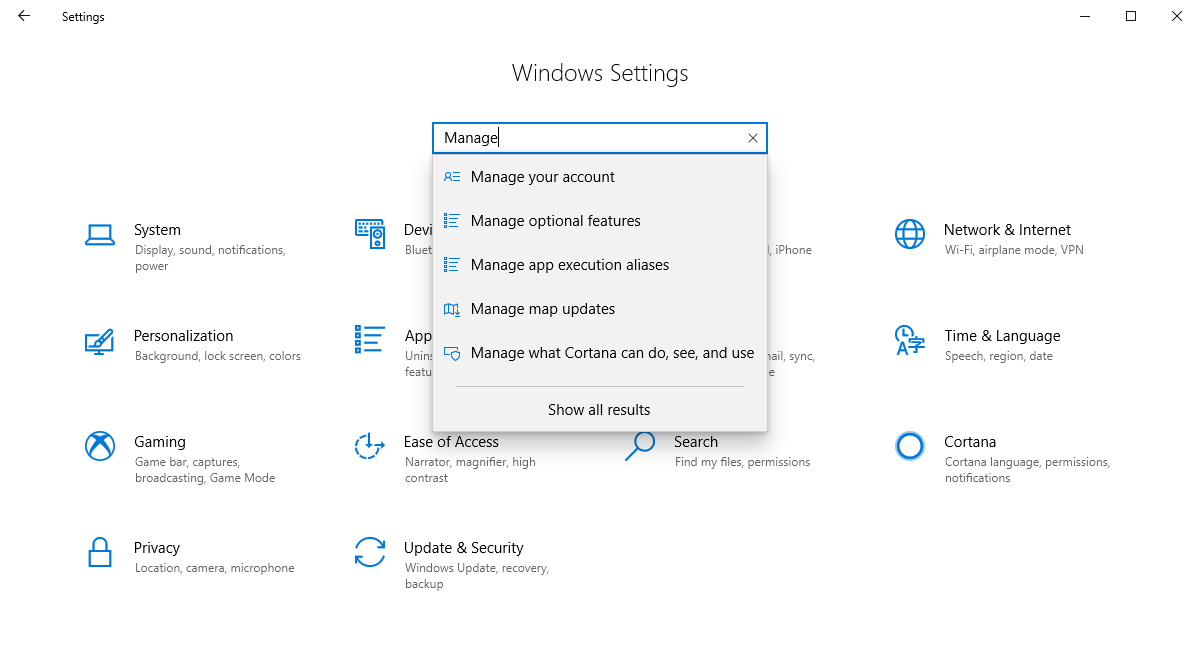


## **Activity 4 –** Remote Active Directory Management

For this activity, you will use two methods to remotely access the Active Directory Server. First, you will install the Remote Server Administration Tool (RSAT) on Windows 10 and then use PowerShell for remote access. Once you can remotely administer Active Directory, the next activity will walk you through creating Organizational Units (OUs), and adding users.

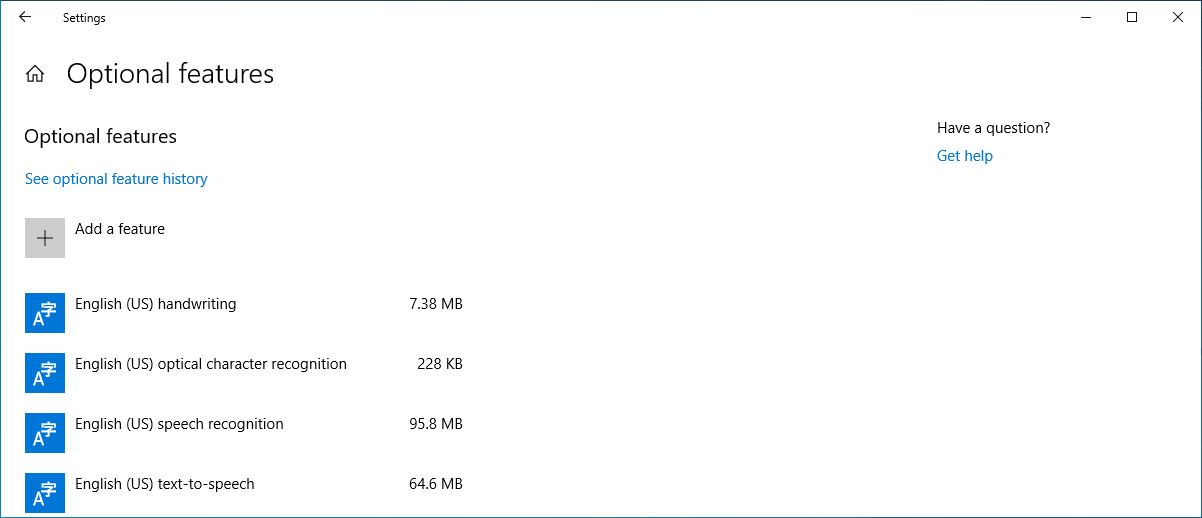
1. From the Windows program menu open “*Settings*” and search for “*Manage Optional Features*,” (Figure 56).

**Figure 56** – Windows Settings



1. From the “*Optional features*,” window click the “*Add a feature*” button, Figure 57.

**Figure 57** – Optional Features

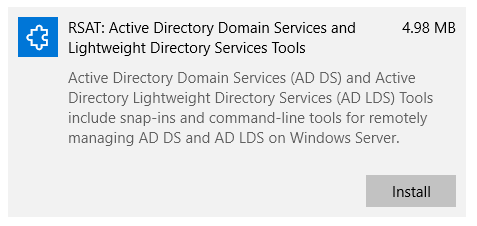


1. In the “*Add a feature”* window (Figure 58), install the following services, RSAT: Active Directory Domain Services and Lightweight Directory Services Tools, RSAT DHCP Server Tools, and RSAT DNS Server Tools (Figures 59 through 61).

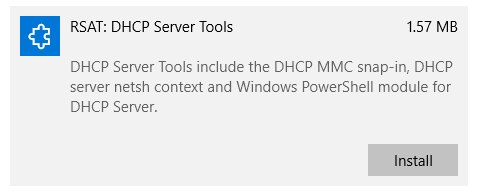
**Figure 58** – RSAT: Active Directory Domain Services and Lightweight Directory Services Tools



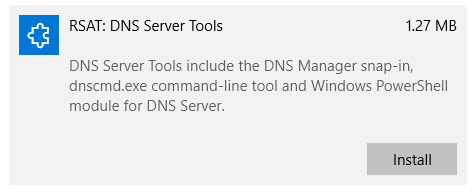
**Figure 59 –** RSAT: Active Directory Domain Services and Lightweight Directory Services Tools



**Figure 60 –** DHCP Server Tools

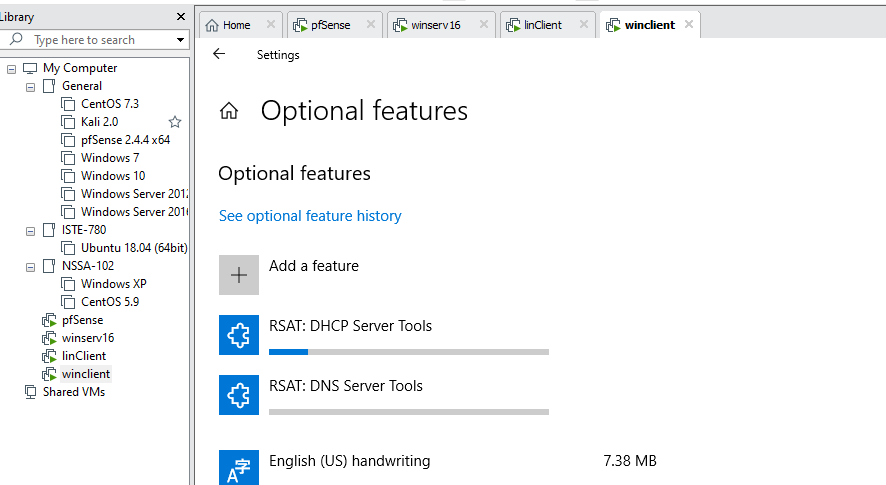


**Figure 61 –** DNS Server Tools



**Be patient while the features are installed!**

**Figure 62** – Windows Features Install



1. Once the install completes open the *Control Panel,* select “*view by small icons”* and click *Administrative Tools* (Figure 63).

**Figure 63** – Control Panel Items

****

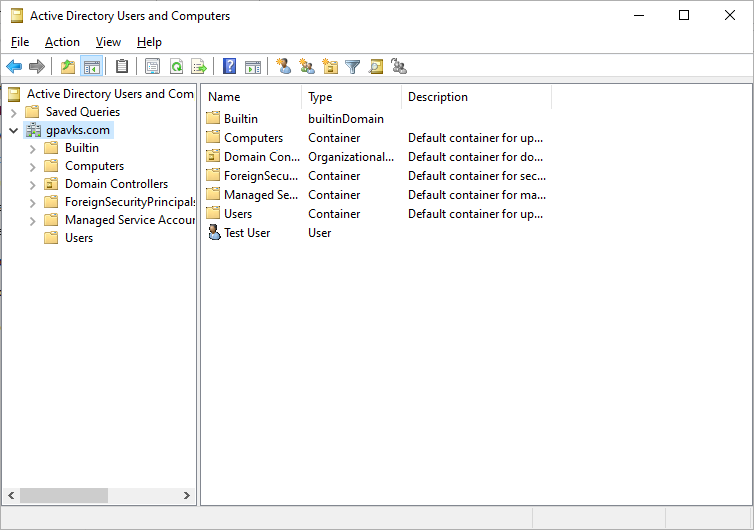
1. Assuming that the features installed correctly you will see a shortcut for “*Active Directory Users and Computers*” Figure 64.

**Figure 64** – Active Directory Users and Computers



1. Double-click “*Active Directory Users and Computers*” to open the Active Directory Users and Computers window. IT will have the same look and feel as if you were opening it on the server.(Figure 65).

**Figure 65** – Active Directory Users and Computers Remote Access



1. To remotely access the server using PowerShell, open Windows PowerShell as an administrator and type the following command, using the hostname of your Active Directory server. In the example provided the hostname is “*winserv.*”



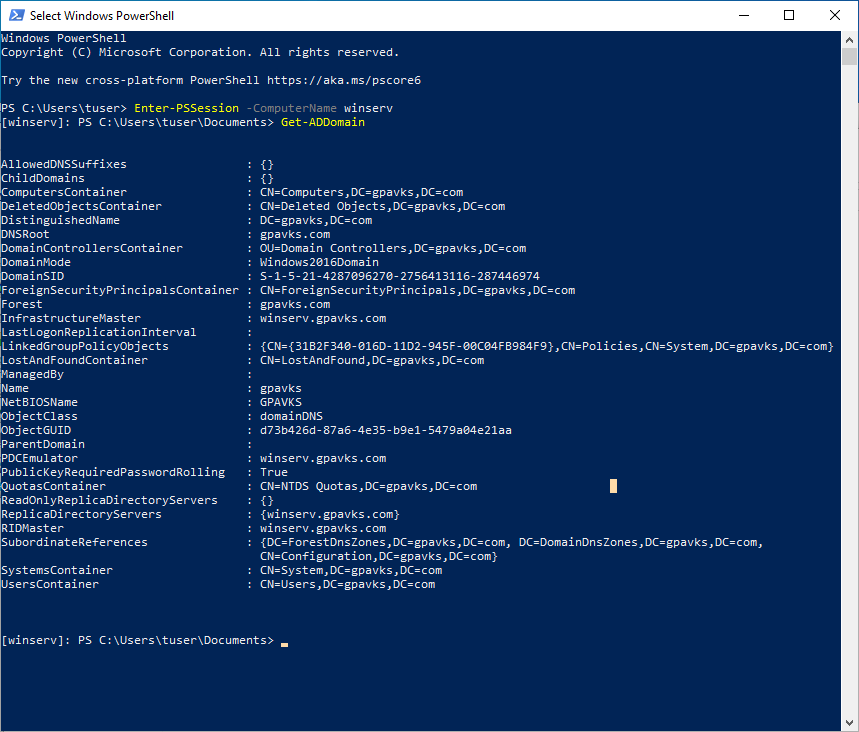
1. We can also use PowerShell to quickly find information about the domain by typing the following command.





For the report, you must provide a **single** screenshot that shows the PowerShell remote session and output from the Get-ADDomain command. Figure 66 provides an example.

**Figure 66** – Sample Screenshot for PowerShell Session and ADDomain Output



## **Activity 5 – Creating Organizational Units and Add Users**

For this activity, you will use the Remote Server Administration Tool (RSAT) from the previous activity to create organizational units and add users to them. Additional tasks will be done remotely using PowerShell.

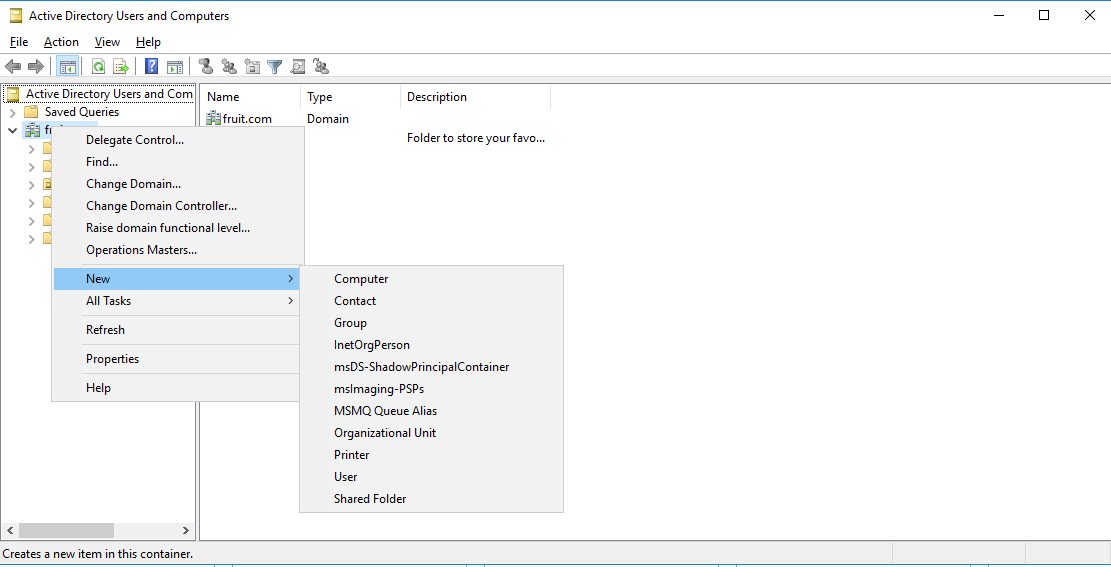
1. Using RSAT and the tools in Active Directory Domain Users and Computers (ADUC) create an Accounting OU inside your domain and add a minimum of four users to it, see Table 1.

**Table 1** – Users in the **Ramones** Organizational Unit

| Joey Ramone  Lead Singer  12-1789 x3456 | Johnny Ramone  Guitarist  34-1797 x3456 |
| --- | --- |
| Marky Ramone  Drummer  23-1801 x5675 | Tommy Ramone  Drummer  Bldg. 34 Office 1809 x5678 |
| Dee Dee Ramone  Bassist  Bldg. 34 Office 1817 x5638 | Linda Ramone  Roadie  Bldg. 12-1837 Ext. 6748 |

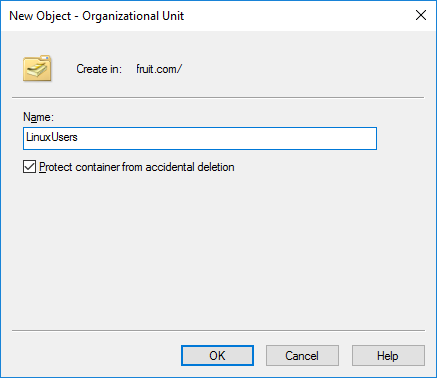
1. Create an organizational unit by right clicking on the domain; and from the dropdown menu select *New 🡪 Organizational Unit* (Figure 67).

**Figure 67** – Adding an Organizational Unit

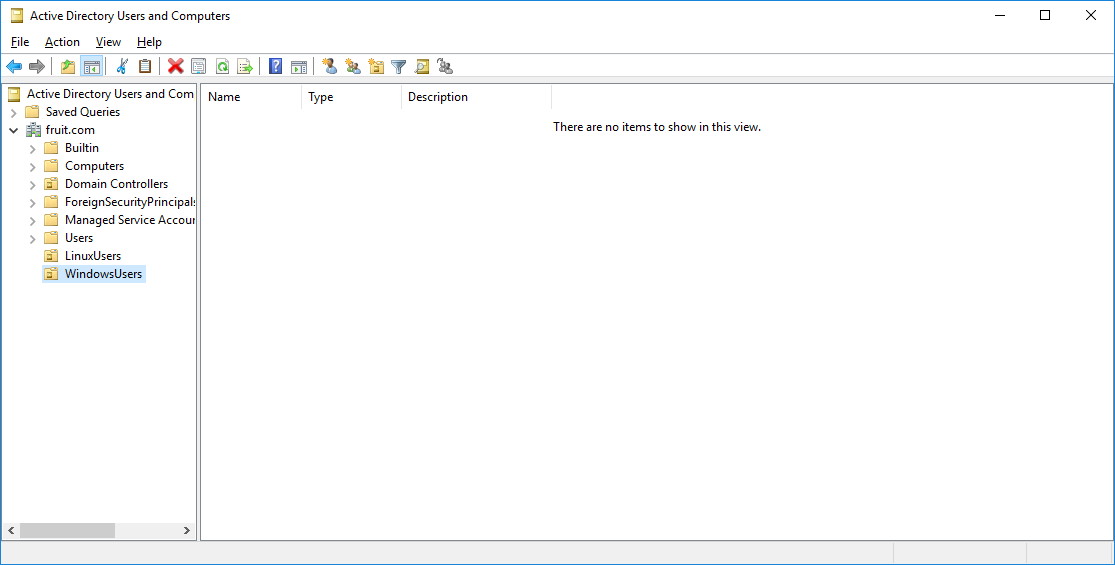


1. To create an organizational unit, enter a name in the *Name* field of the *New Object – Organizational Unit wind*ow (Figure 68) and click ***OK***. When you have completed this step, the Organizational Unit will appear in domain in Active Directory Users an Computers (Figure 69).

**Figure 68** – New Object – Organizational Unit

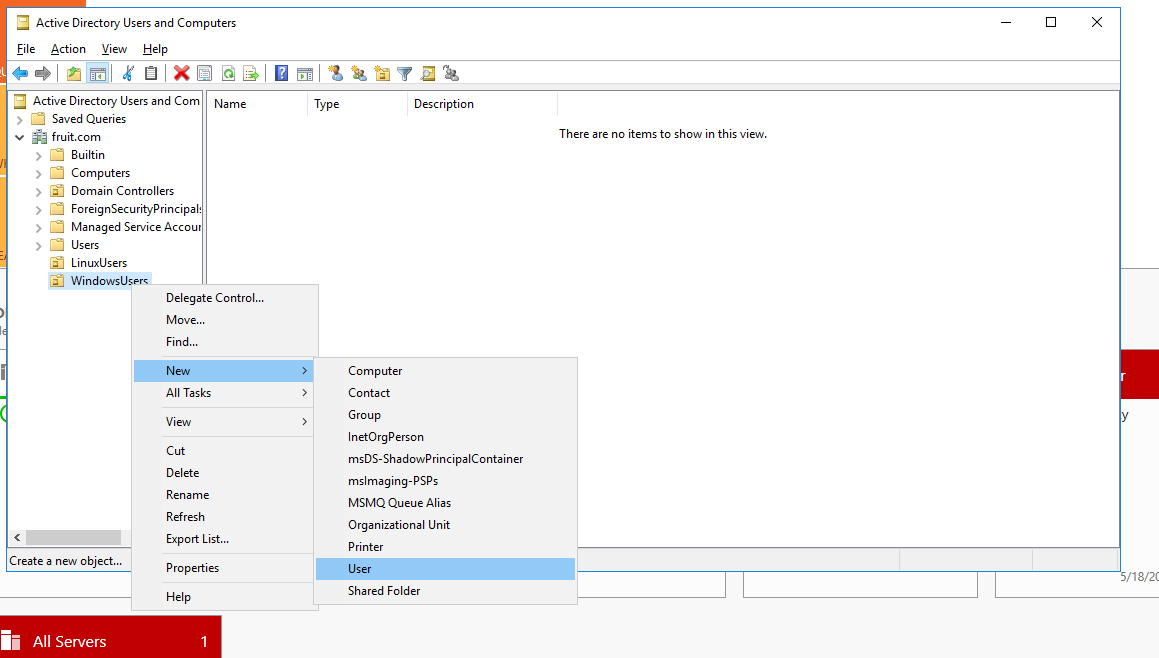


**Figure 69** – Updated Active Directory Users and Computers



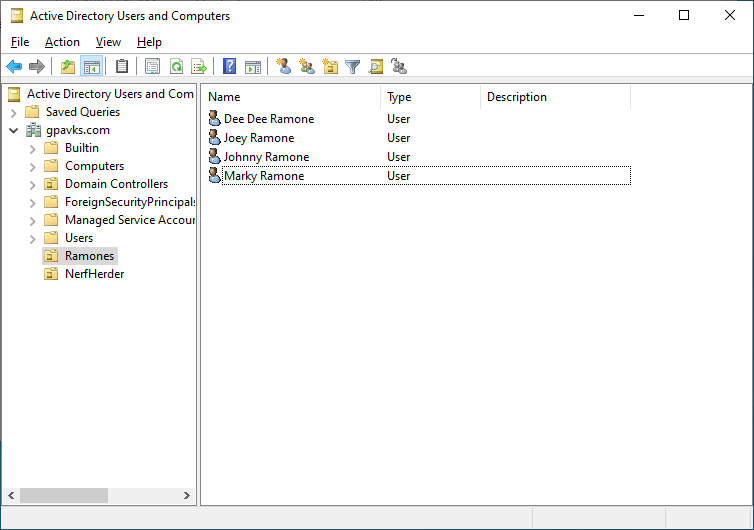
1. Next add a user to the Organizational Unit by right clicking on the OU and from the dropdown menu select ***New*** and then ***User***, see Figure 70.

**Figure 70** – Adding a User to the Organizational Unit



1. Repeat the process to add four additional users to the Organizational Unit. When complete it will look similar to the information in Figure 71.

**Figure 71** – Created User in Organizational Unit



1. Use PowerShell to create a second Organizational Unit in your domain with four new accounts. You may use the information in Table 2.

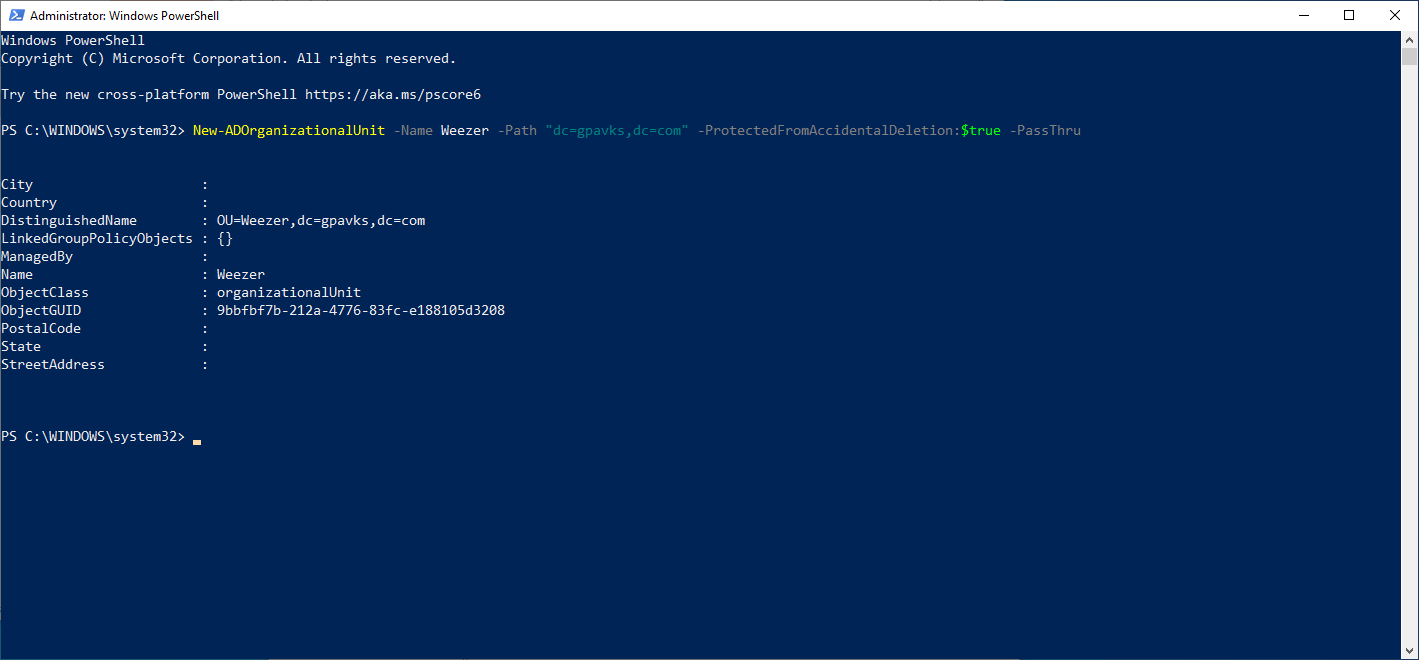
**Table 2 –** Users in the **Weezer** Organizational Unit

| Rivers Cuomo  Lead Guitar  Bldg. 57-1841 Ext. 5624 | Patrick Wilson  Drummer  Ext. 6745 Bldg. 21-1841 |
| --- | --- |
| Brian Bell  Vocals  Ext. 6734 Bldg. 52-1845 | Scott Shriner  Bassist  Ext. 5197 Bldg. 54-1849 |

1. To create the Organizational Unit, use the following command (one line). The LDAP identifier “dc”, is for “domain component,” which will be covered later in the semester, for now just understand that it is being used to define the domain in Active Directory. The output will look similar to Figure 72.



**Figure 72** – Organizational Unit Creation Using PowerShell



1. To add a user to the Organizational Unit, use the following command (one line). Remember to substitute your domain information.



1. Repeat the command to add additional users to the Organizational Unit.
2. To add other attributes to the user accounts, use the Set-ADUser cmdlet. The following example, adds the extension to the “OfficePhone” attribute for the user, Patrick Wilson.



1. Using the Set-ADUser identifies the distinguished name of the AD object. There are generic parameters that are passed to the Set-ADUser cmdlet that can be used to modify the account. Below is a summary, for more information refer to the Microsoft documentation.

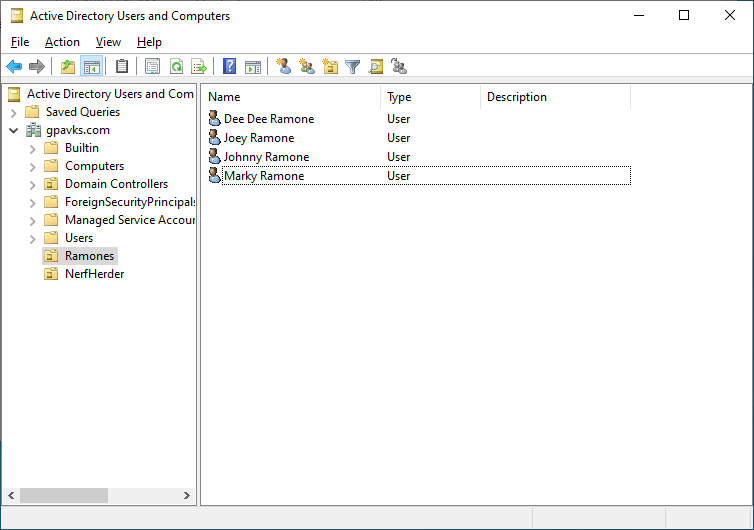
* Add – adds one or more values to a property
* Clear – clears all values of a property
* Remove – removes one or more values from a property
* Replace – replaces the values of a property





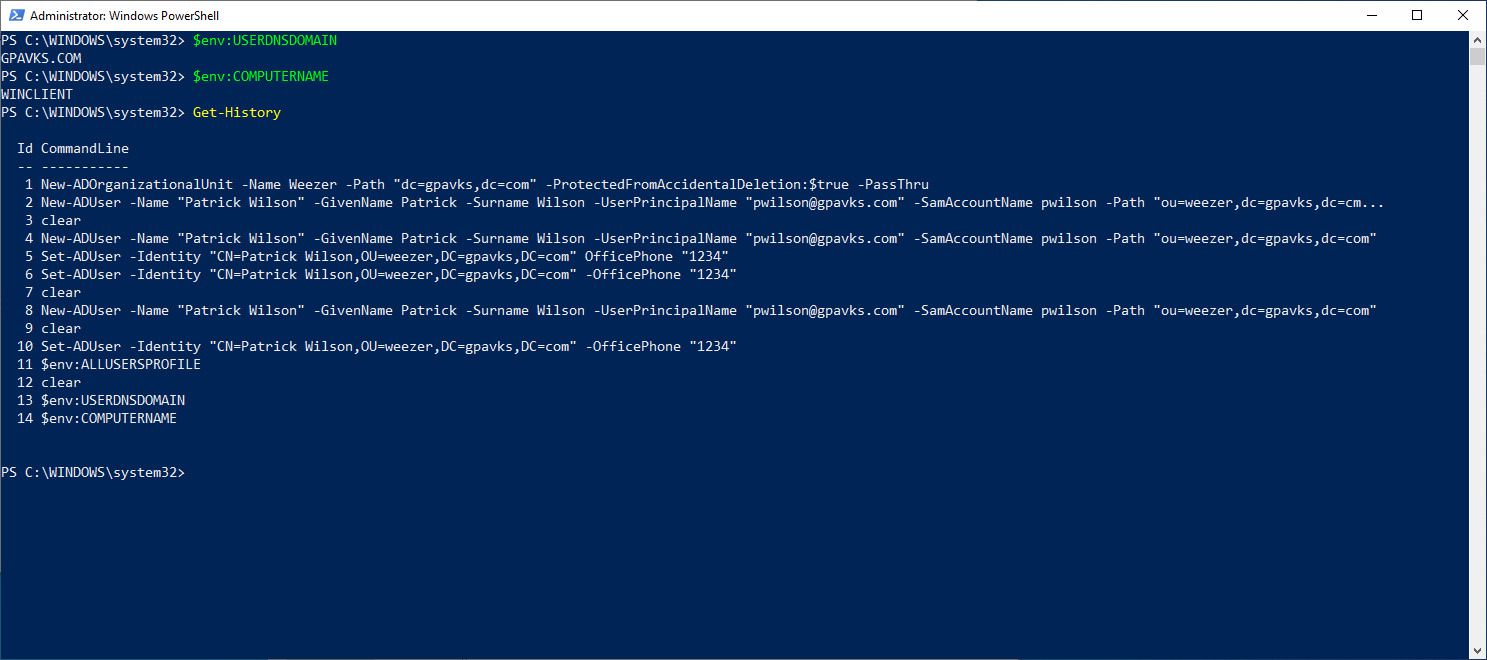
You must provide **TWO** screenshots of the information in the Active Directory Users and Computers. It must show the domain and the users created for **BOTH** Organizational Units, see Figure 73 for an example.

**Figure 73** – Organizational Unit and Users Sample Screenshot



You must provide a screenshot of the PowerShell history. It must show the creation of at least one user and include the domain and the hostname of the computer (Figure 74). Use $env:USERDNSDOMAIN, $env:COMPUTERNAME, and the Get-History cmdlets. You may split the screenshots if necessary.

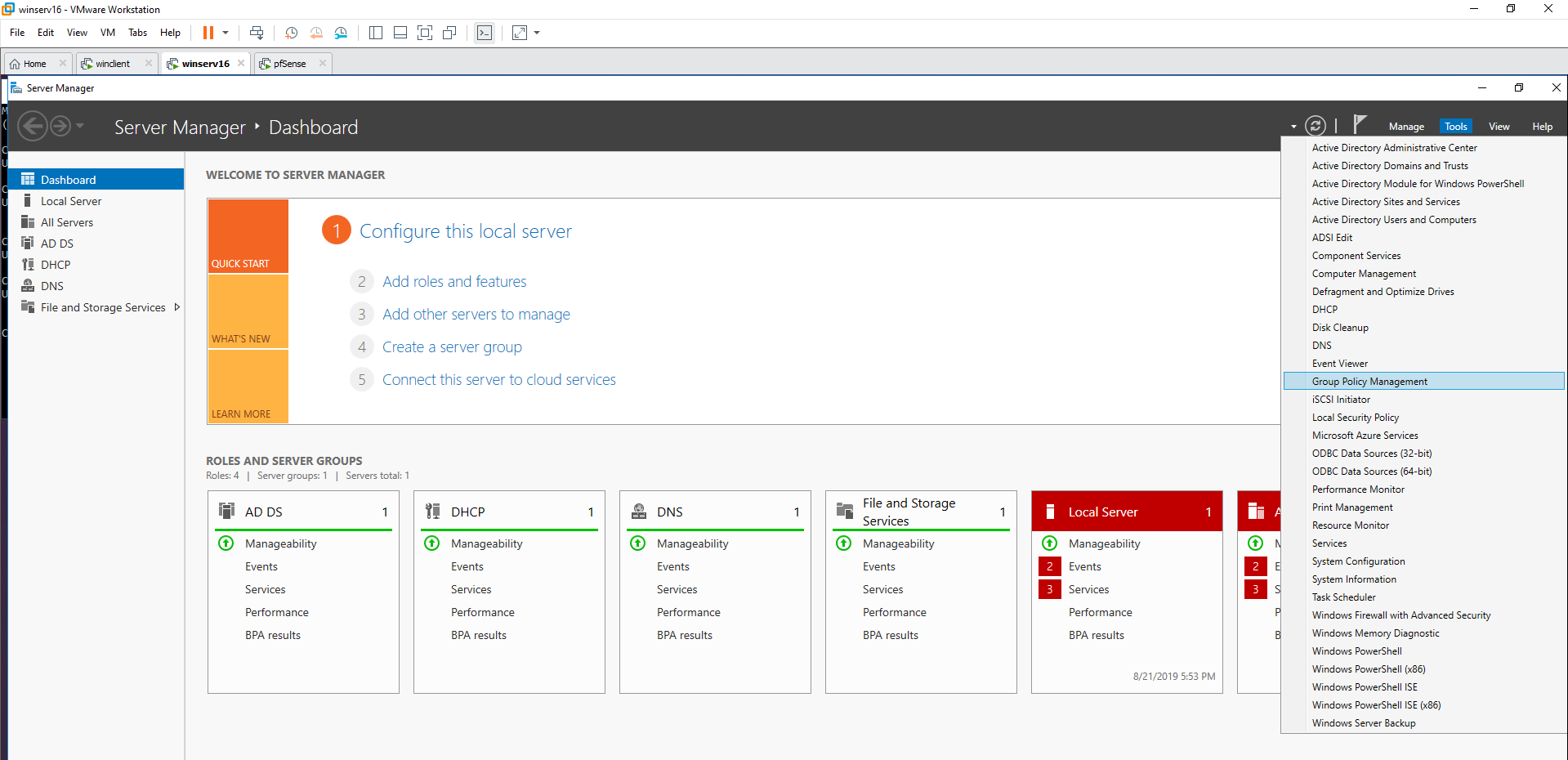
**Figure 74** – Sample PowerShell History



## **Activity 6 – Creating and Linking a Group Policy Object**

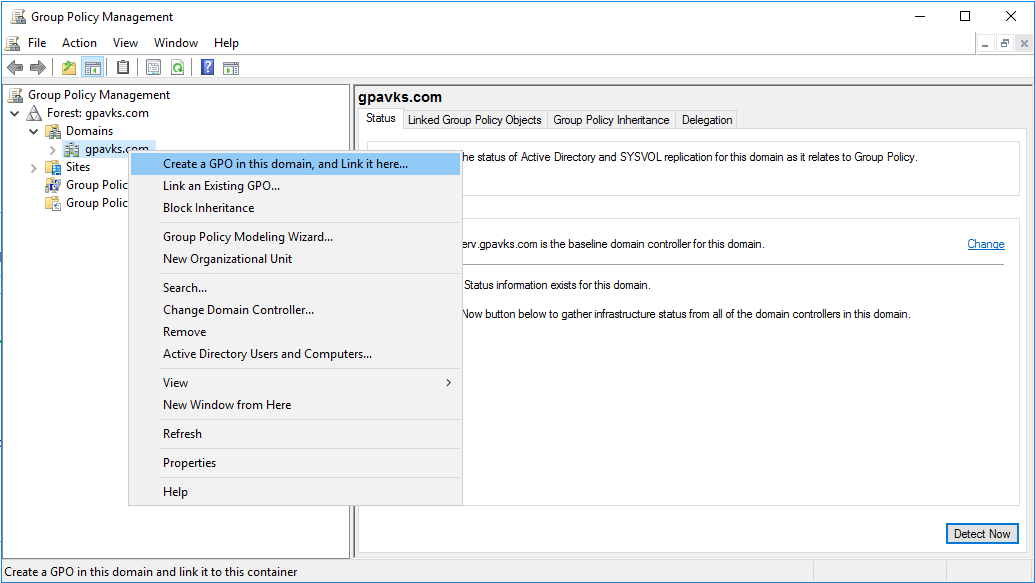
1. From the Server Manager Dashboard select *Tools* 🡪 *Group Policy Management* (Figure 75).

**Figure 75** – Group Policy Manager



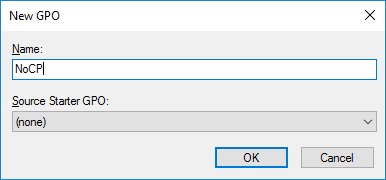
1. Right-click on the domain and select “*Create a GPO in this domain, and Link it here…*” (Figure 76).

**Figure 76** – Creating a GPO



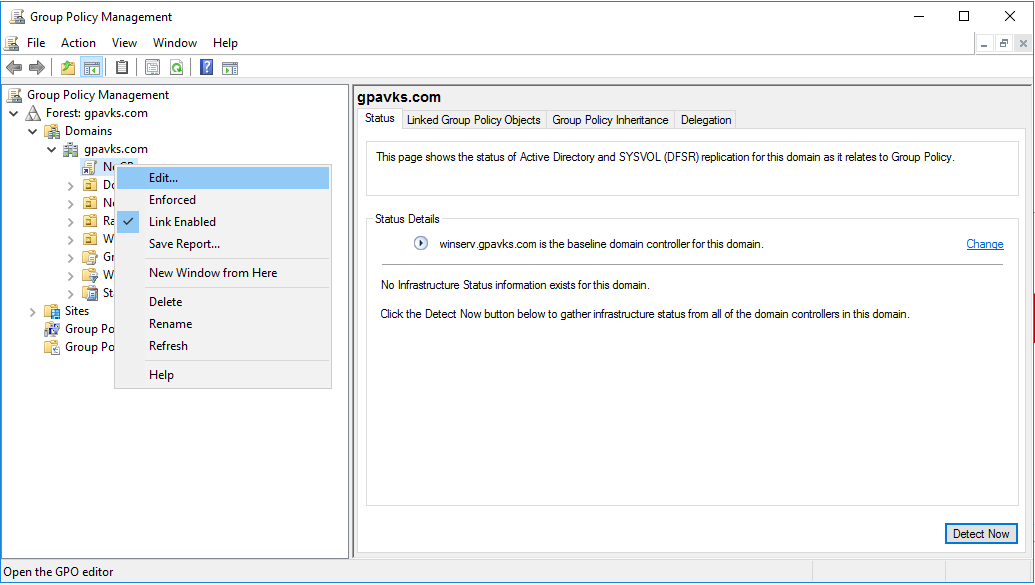
1. In the New GPO window, enter a name. In the example provided (Figure 77), I’m using “*NoCP*,” for no Control Panel. Name it whatever you like and click ***Ok***.

**Figure 77** – New GPO



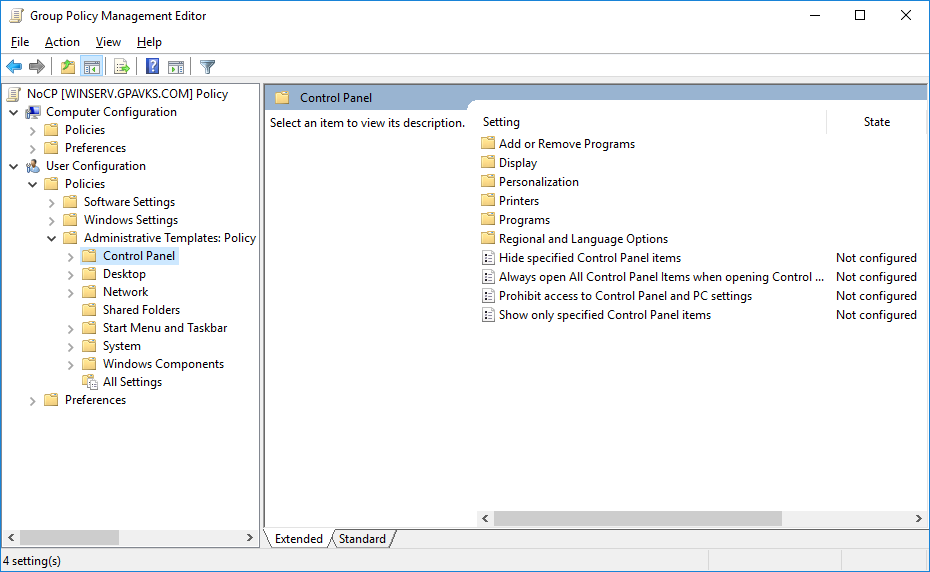
1. Right-click on the GPO you just created and select ***“Edit”*** from the dropdown menu (Figure 78).

**Figure 78** – Edit the GPO



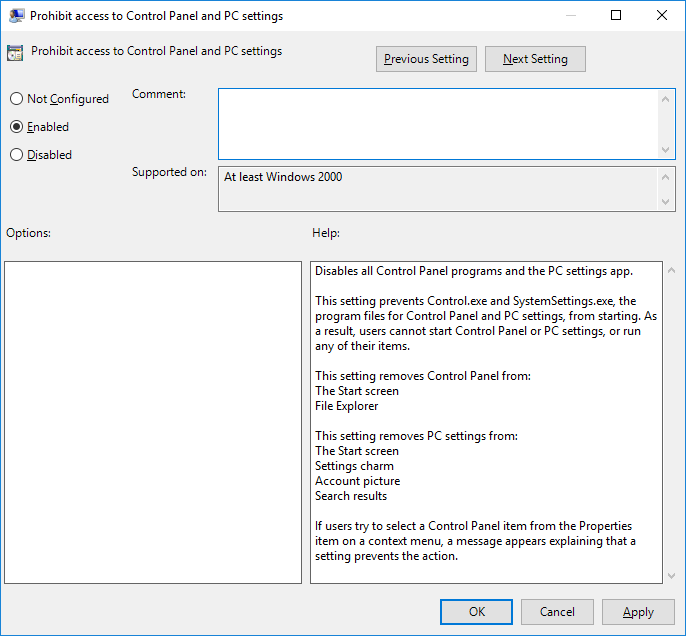
1. Next, navigate to *User Configuration 🡪 Policies 🡪 Administrative Templates*, and the Control Panel folder. In the right pane, double-click “*Prohibit access to Control Panel and PC settings*” (Figure 79).

**Figure 79** – Configuring GPO



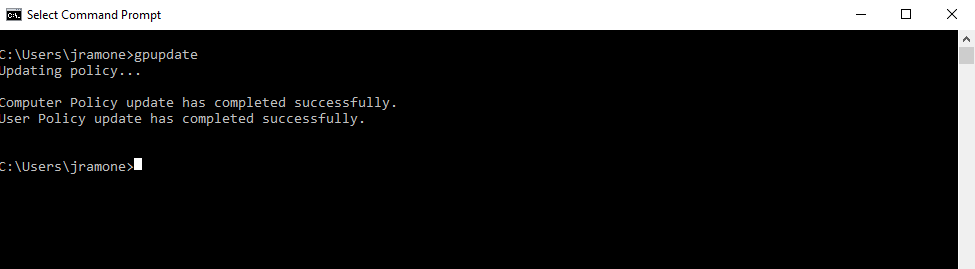
1. Select “*Enabled*”, click ***Apply*** and then ***OK*** (Figure 80).

**Figure 80** – Enable GPO



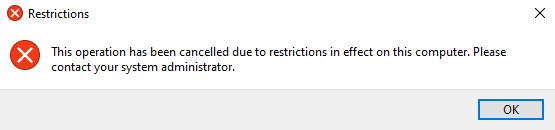
1. Return to the Windows 10 client and login in using a domain user account. Do not use and account if the user is a member of the domain admin group, remember the domain admin inherits the local policies so the GPO you just created only applies to domain users.
2. Open the Command Prompt and type the command gpupdate to update the policy for that user (Figure 81).

**Figure 81** – Group Policy Update



1. At this point the user will not have access to the control panel and receive the following message (Figure 82).

**Figure 82** – Group Policy in Effect





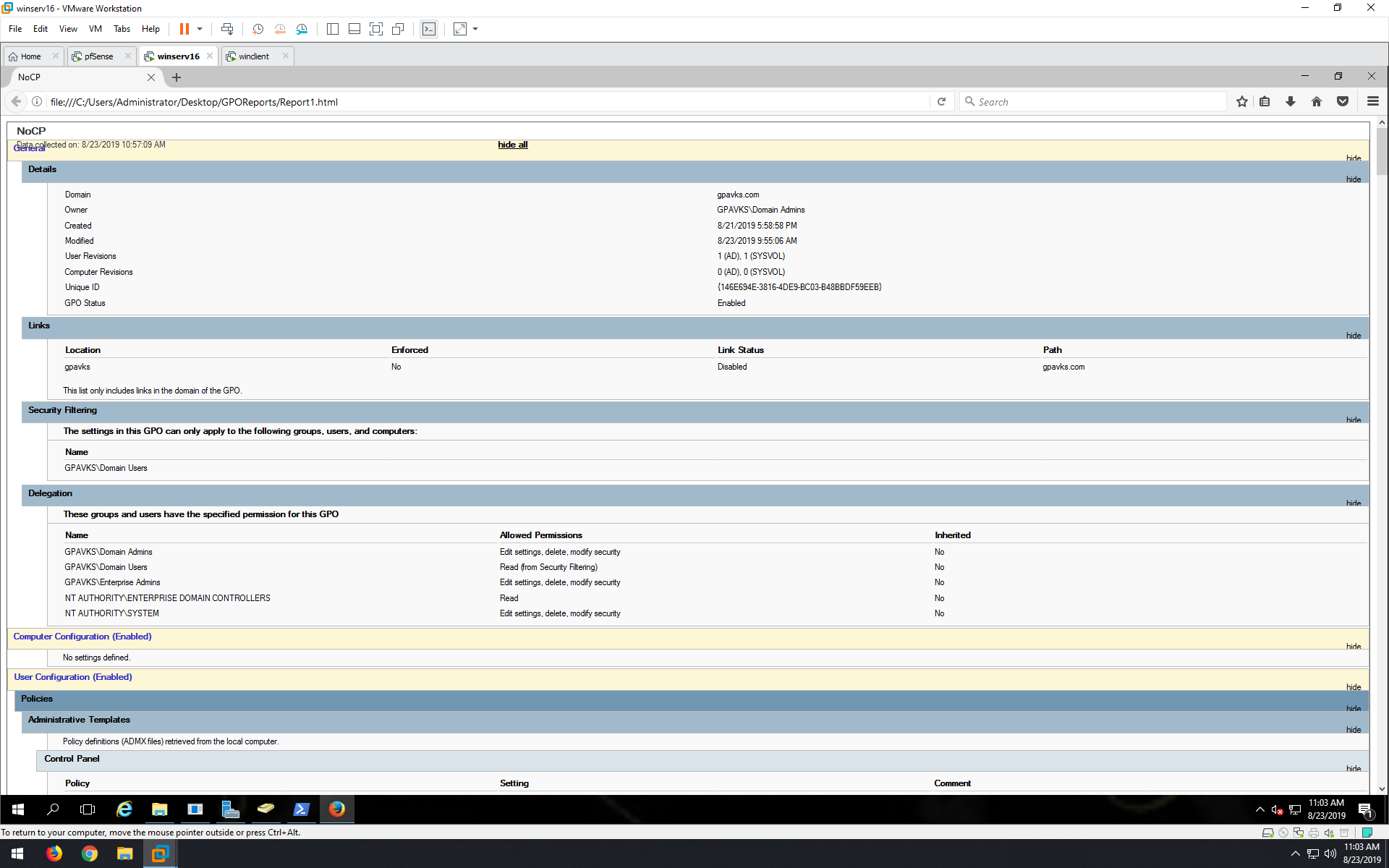
It’s relatively common for companies to use a standard desktop wallpaper across all workstations in the organization. For this exercise, you will create a GPO that does this for one of the organizational units created in the lab. Because you are creating a GPO for the Organizational Unit, it is important to understand GPO precedence, make sure to read the article posted to myCourses. If you are looking for some help, this YouTube video should do the trick.

https://www.youtube.com/watch?time\_continue=93&v=8kCjK9wiN-Y

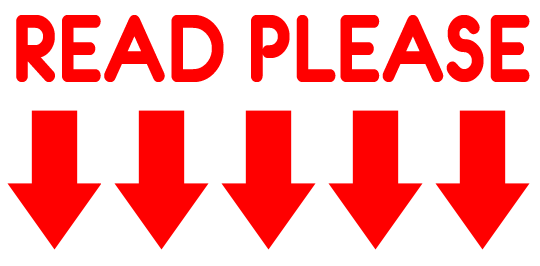
**For the report include a screenshot showing the Group Policy Reports.** Using Windows documentation create a report that shows the GPOs created in the lab. Refer to Figure 83 for an example. Make sure to show both GPOs and use multiple screenshots if necessary. Append a letter to the figure, for example “***Figure 8a – NoCP GPO Report***.” Make sure to include the details section.

Windows Resource - <https://docs.microsoft.com/en-us/powershell/module/grouppolicy/get-gporeport?view=win10-ps>

**Figure 83 –** GPO Report Example



# **Screenshot Summary**



All screenshots for Lab 01 must be included in the report. For each missing screenshot, you will receive a 5% penalty on the report grade. If your screenshots do not include the required information, are illegible, blurry, or otherwise unreadable, you will not receive credit. Any attempt to alter the information in the screenshots is academic dishonesty, and you will receive a zero grade for the report.

**All screenshots must be labeled in the report, using the following titles.**

Figure 1 – Active Directory and DHCP Server Information

Figure 2 – Windows 11 Network Configuration Information

Figure 3 – Windows 11 Domain Information

Figure 4 – Windows 11 Network and Domain Verification

Figure 5 – Rocky Linux Verification

Figure 6 – PowerShell Get-ADDomain Output

Figure 7 – First Organizational Unit\*

Figure 8 – Second Organizational Unit\*

Figure 9 – PowerShell History

Figure 10 – GPO Report\*

\*If you need multiple screenshots for the GPO reports just append a letter, for example, Figure 8a, Figure 8b.