NSSA221 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 computing environment. 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 company's 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 understand 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 2025, 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 2025.
- 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 with an organization's structure.
- Manage user accounts in Active Directory using PowerShell and Active Directory Users and Computers, or ADUC.

Preparation

- Complete Week 2 readings.
- Review Active Directory presentation.
- Attend class so you do not miss the demonstration.

Activity Summary

Activity 1 – Install and Configure Windows Services
Activity 2 – Create a User Account
Activity 3 – Joining User to the Windows Domain
Activity 4 – Remote Management
Activity 5 – Creating Organizational Units and Adding Users
Activity 6 – Creating and Linking a Group Policy Object

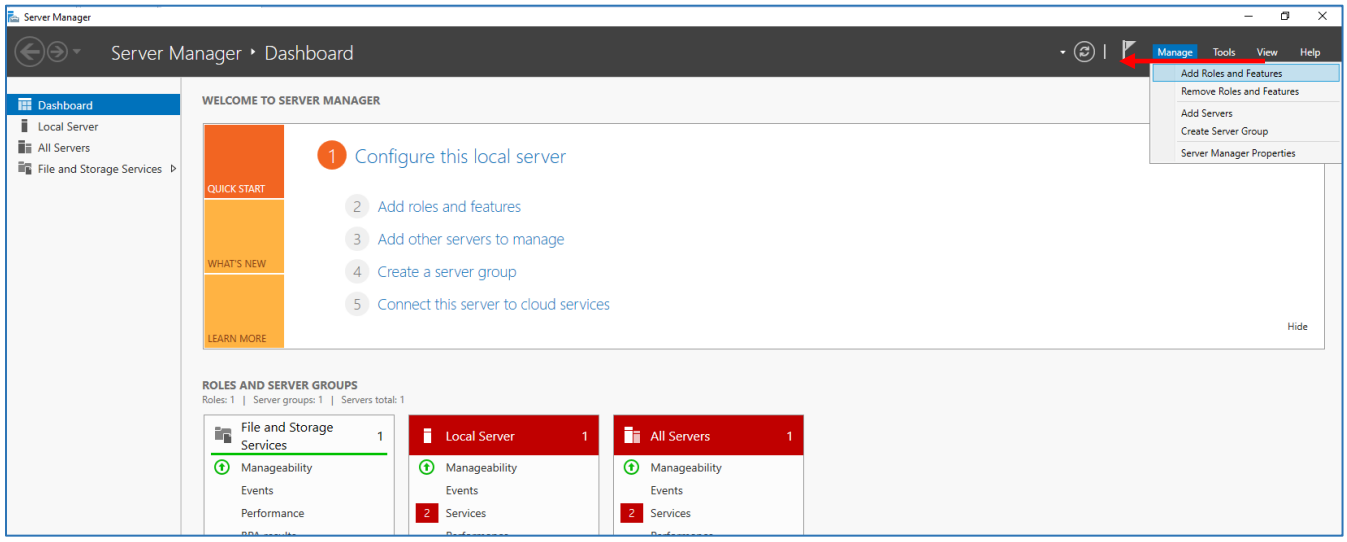
Activities

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 2025 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 Windows Administrative Center and PowerShell.

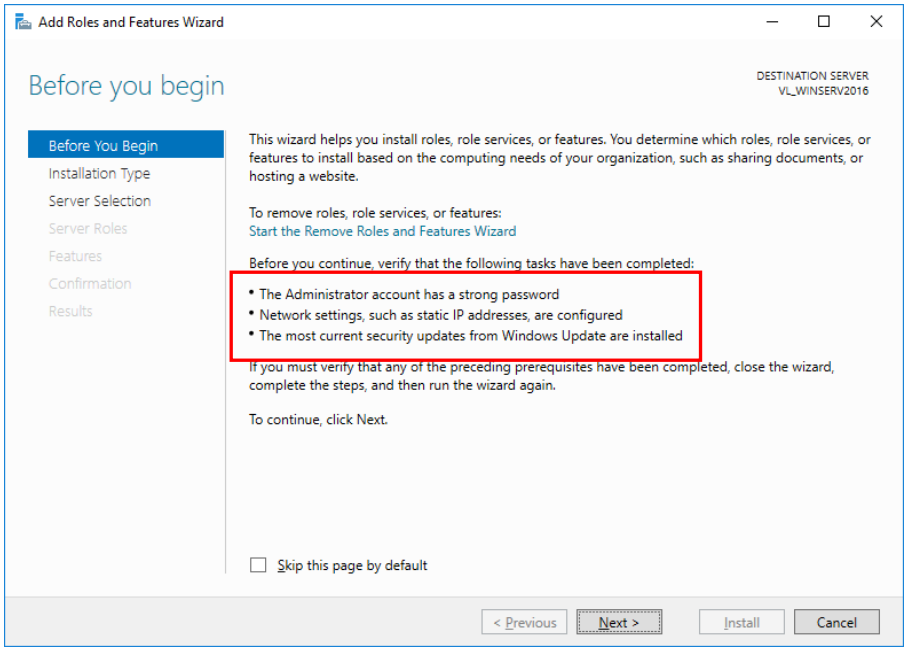
a. From *Server Manager → Dashboard,* select Manage and then "*Add Roles and Features*" to launch the wizard (Figure 1).

Figure 1 – Add Roles and Features



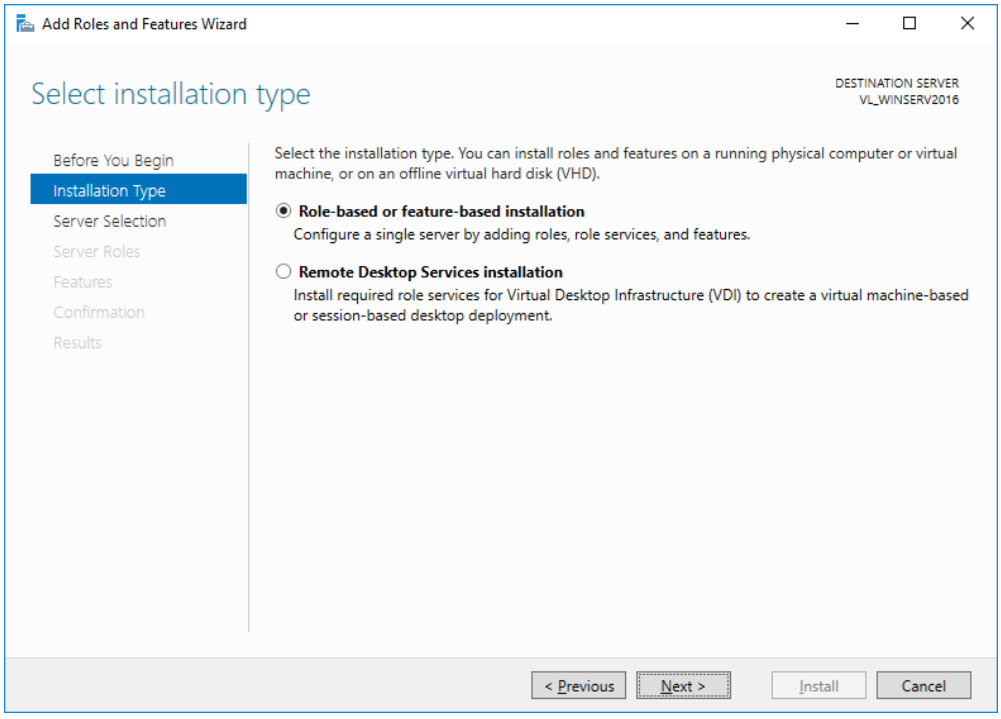
b. The first window will ask you to verify that certain tasks have been completed before you begin the installation (Figure 2). The Windows Server should have its network configuration statically assigned and a hostname from Lab 1. Click ***Next***.

Figure 2 – Before you Begin



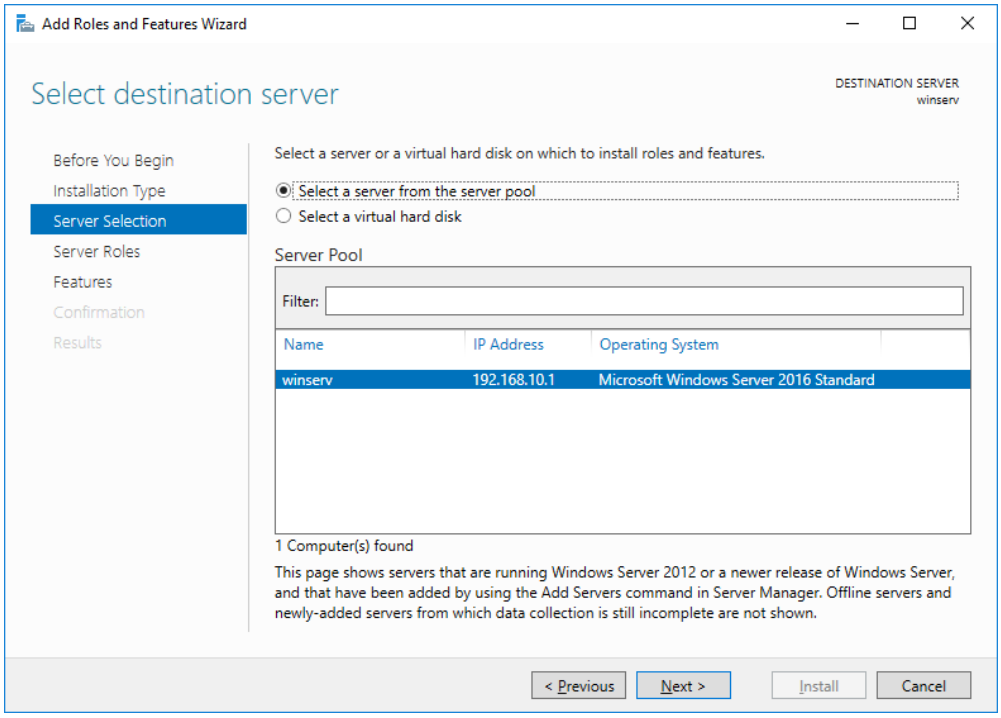
c. The next screen (Figure 9), will prompt you for the installation type, select "*Role-based or feature-based installation*," and click ***Next***.

Figure 3 – Select Installation Type



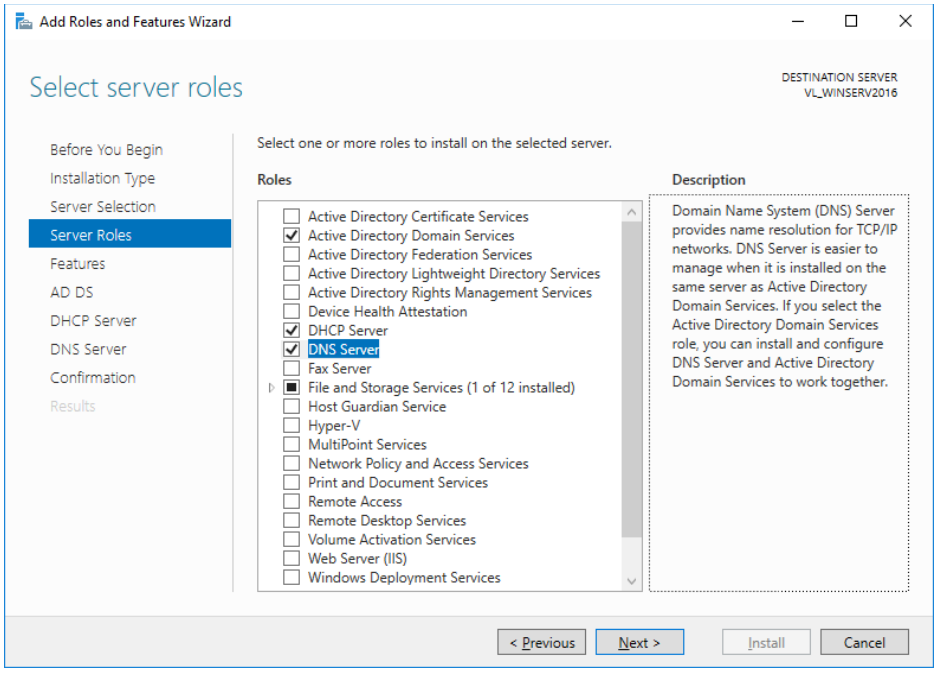
a. The next screen (Figure 4) will ask you to select the server, since this is the only server, you currently have it will be selected by default. Nevertheless, you should see the hostname and static IP address that was configured in Lab 1. Your hostname and IP address may be different from the screenshot. Click ***Next***.

Figure 4 – Select Destination Server



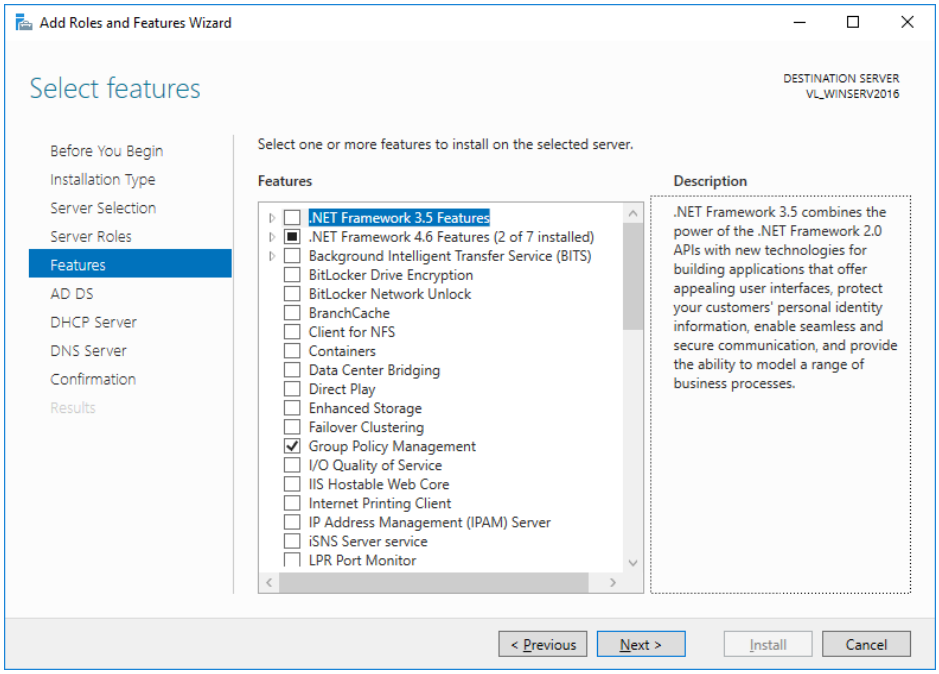
b. The next window (Figure 5) is where you select the three services (roles), *Active Directory Domain Services*, *DHCP Server*, and *DNS Server*. For each service, you are prompted to Add Features, select the default features for each service. Once, all three roles have been selected hit ***Next***.

Figure 5 – Select Server Roles



c. 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***.

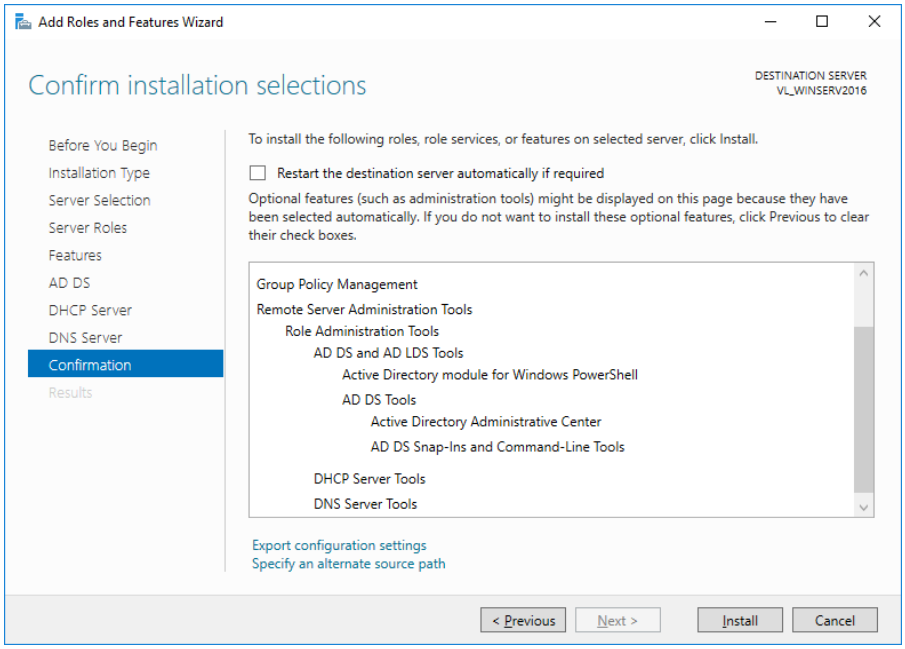
Figure 6 – Select Features



d. The next three windows will provide information about the services being installed, you can read the information or click ***Next***.

e. 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



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

Figure 8 – Installation Progress

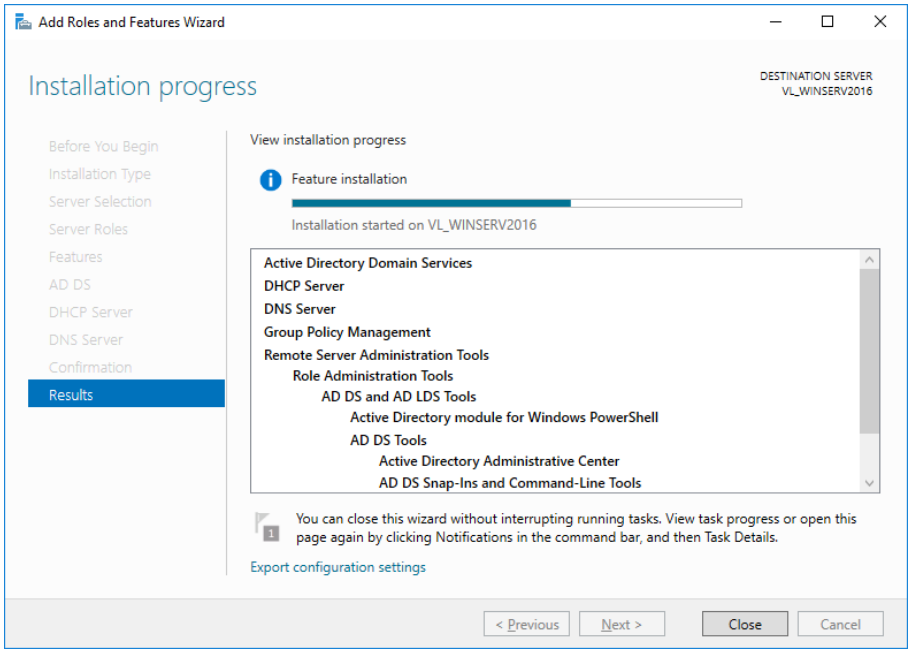
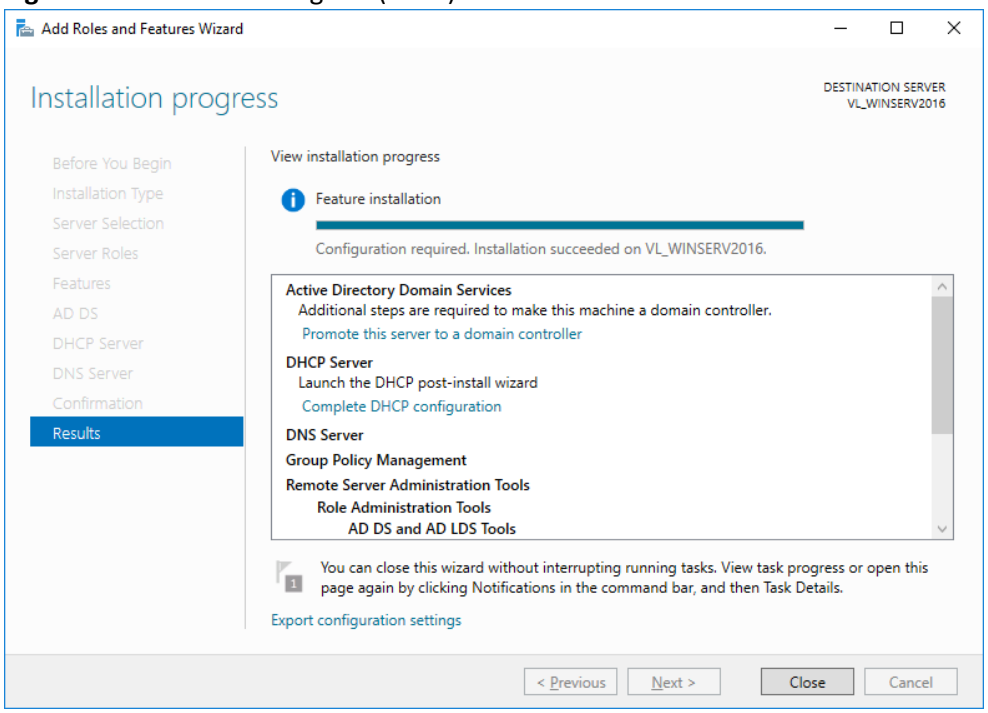
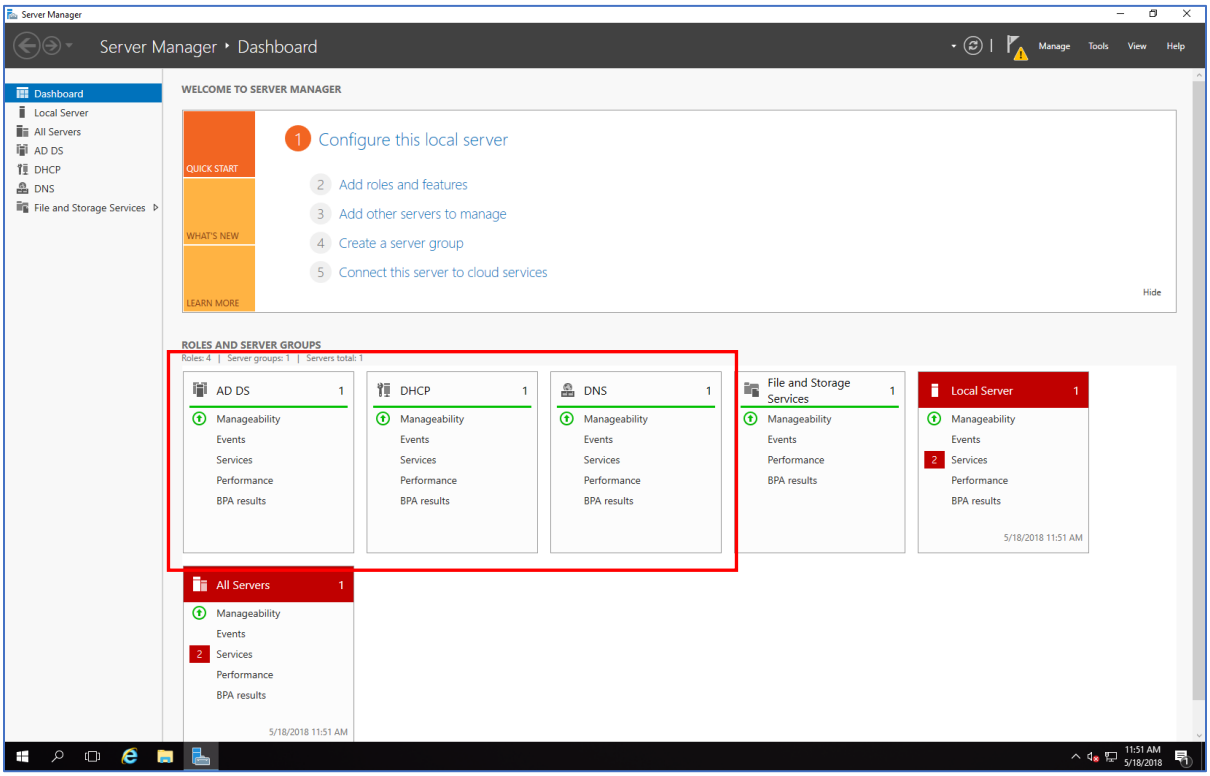


Figure 9 – Installation Progress (cont.)



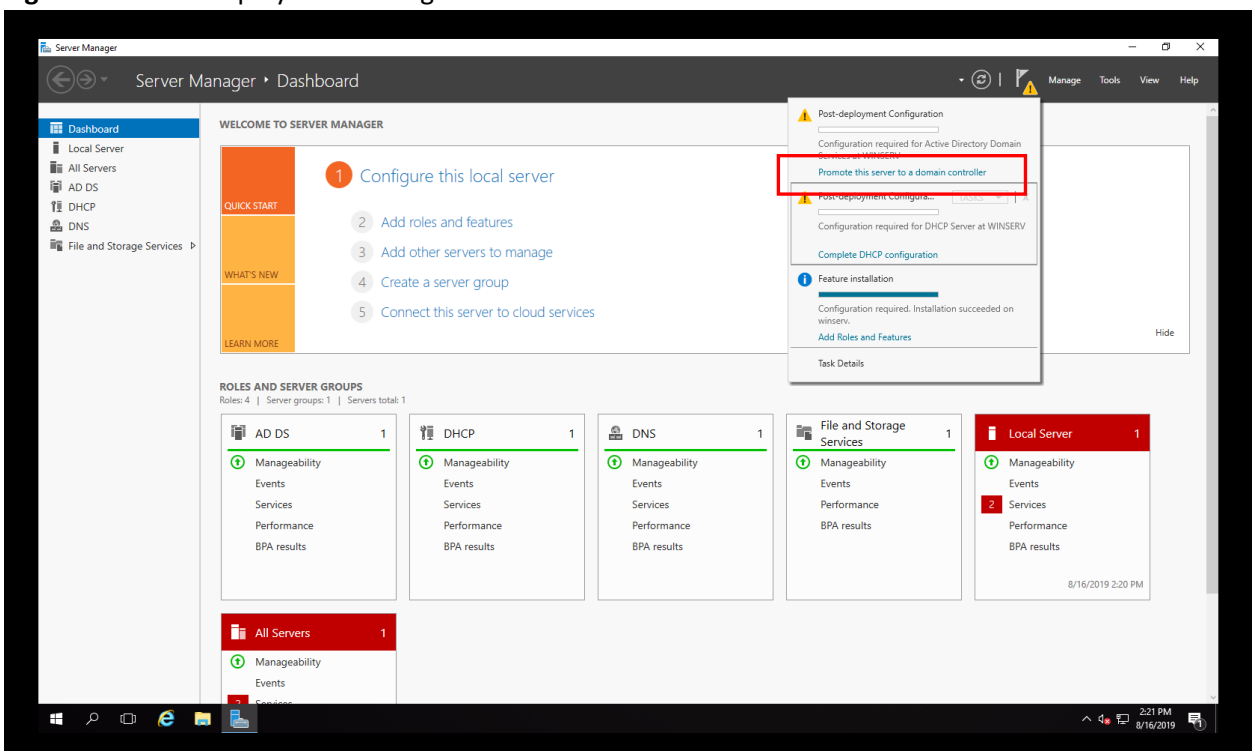
g. When the installation is complete you will see the new services available in the *Server Manager → Dashboard* (Figure 10).

Figure 10 – Post Install Server Manager Dashboard



h. 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



****

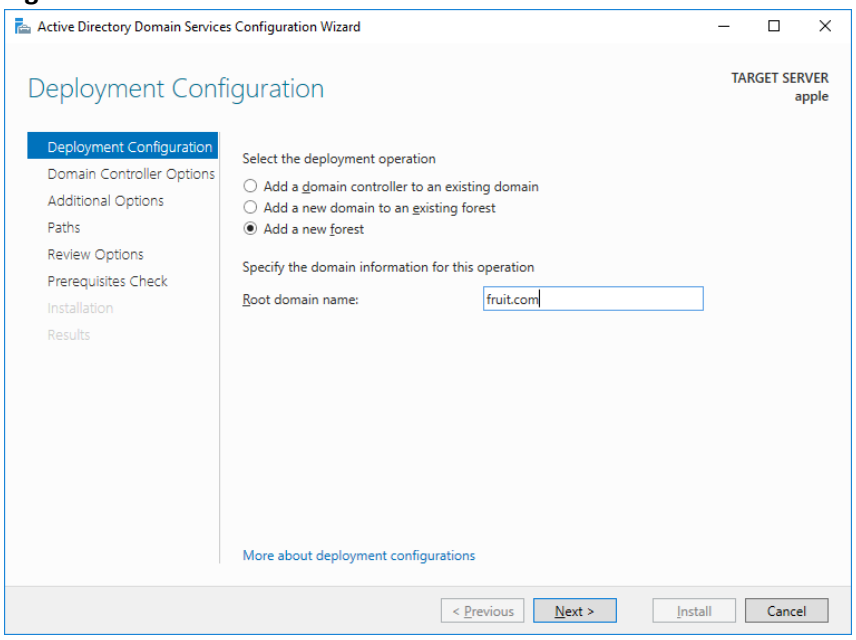
Please Read! Please Read! Please Read! Please Read! Please Read!

****

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! Your ID is the same ID you use to log into myCourses.

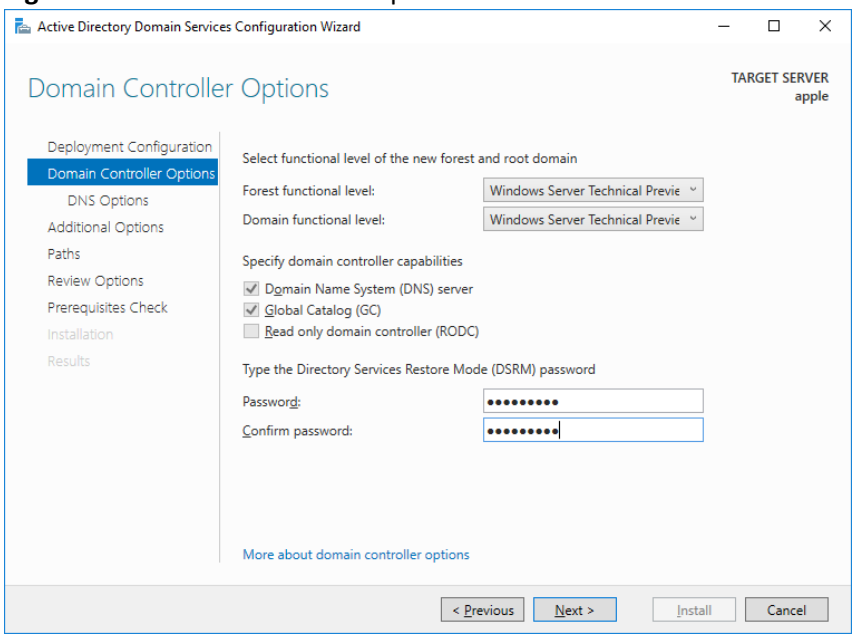
i. Select the "*Add a new forest*" radio button and enter your forest, i.e., your organizations' domain (Figure 12). Your forest must be your student ID followed by ".com." For example, *abc1234.com*. Click, ***Next***. **Do not use the example in the screenshot, it is only there for reference.**

Figure 12 – Add a New Forest



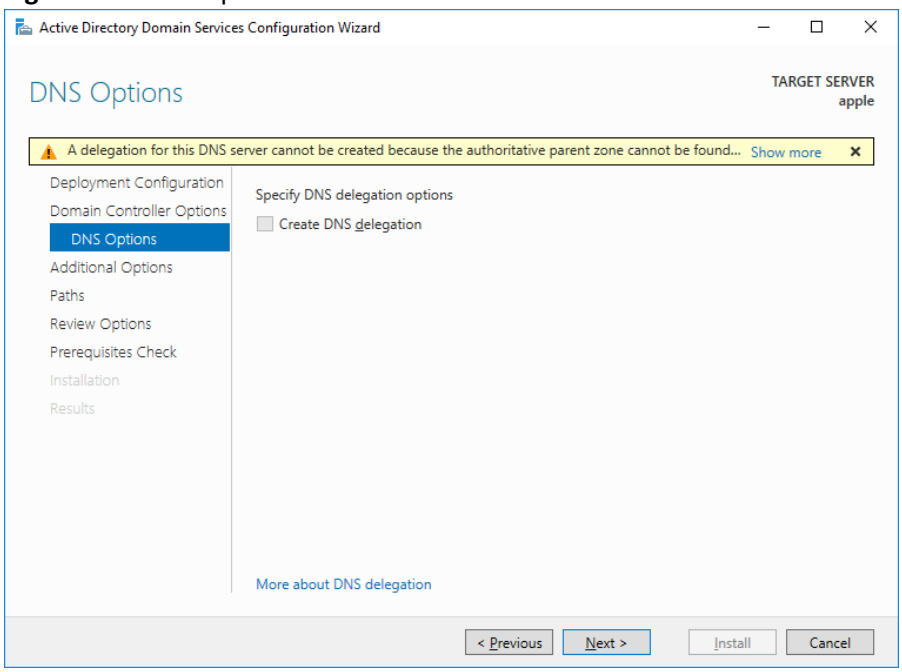
j. On the next screen (Figure 13) enter the password for the Directory Services Restore Mode (DSRM), chances are you will not be needing this but you may want to record the password nonetheless. Click, ***Next***.

Figure 13 – Domain Controller Options



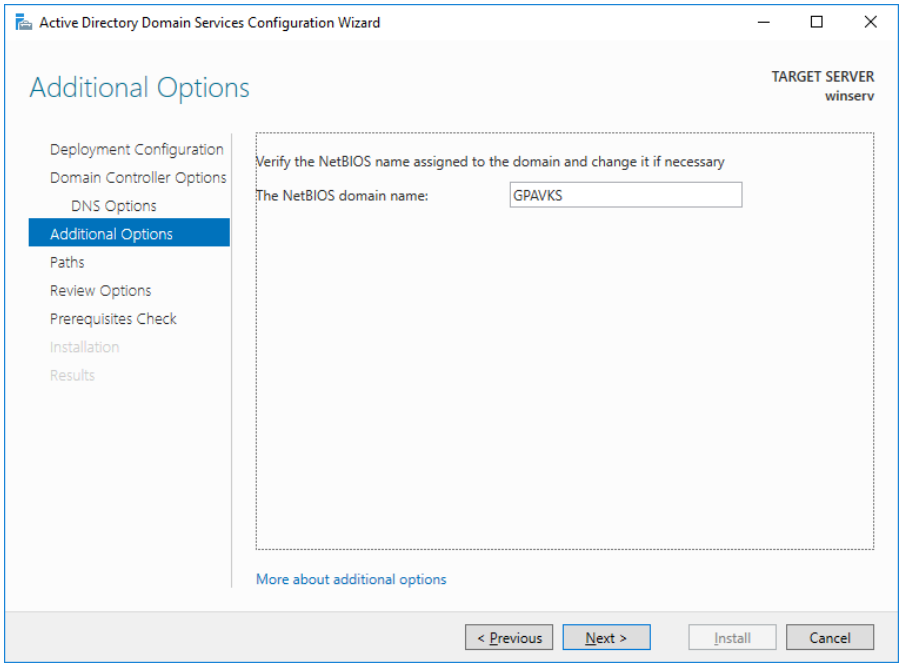
k. On the next screen (Figure 14), you are asked to create a delegation, since we are not registering the domain with a registrar, there is nothing to delegate (you'll learn about DNS delegation in NSSA245), ignore the caution and click ***Next***.

Figure 14 – DNS Options



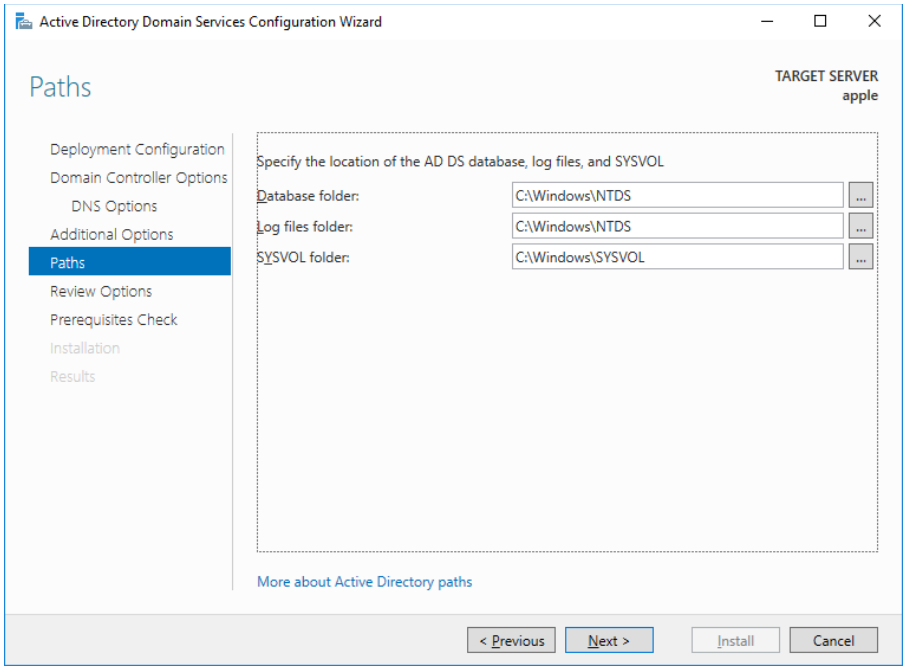
l. The next screen (Figure 15) will ask for the NetBIOS domain name, wait for a moment for it to auto-populate and click ***Next***. **DO NOT** edit the NetBIOS name, it will be your domain in uppercase minus the ".com," this is to be expected. It is simply there for backward compatability.

Figure 15 – Additional Options



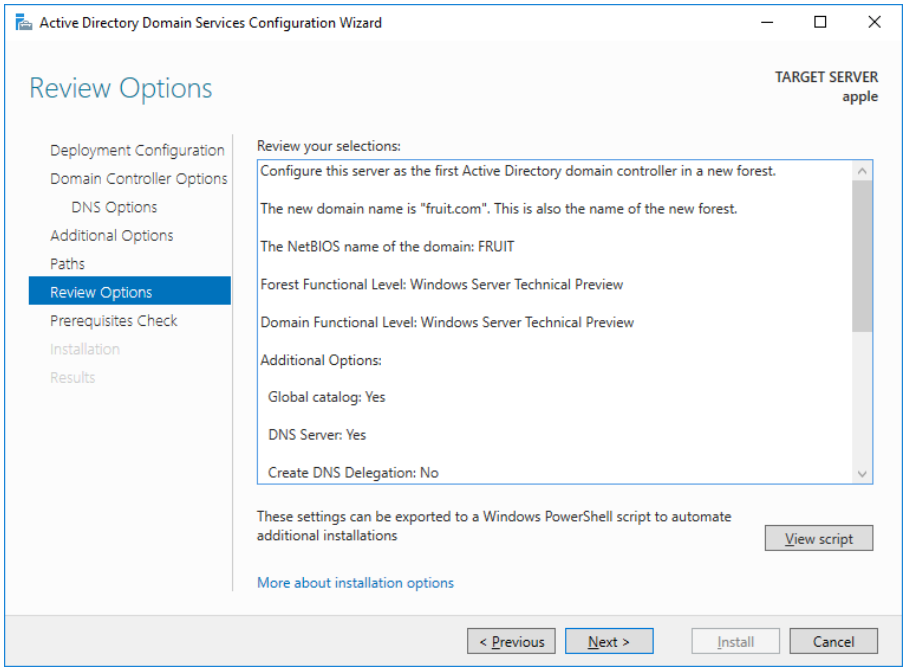
m. The next screen (Figure 16) will ask where you want to locate the ADDS database, log files, and SYSVOL, use the defaults and click ***Next***.

Figure 16 – Default Paths



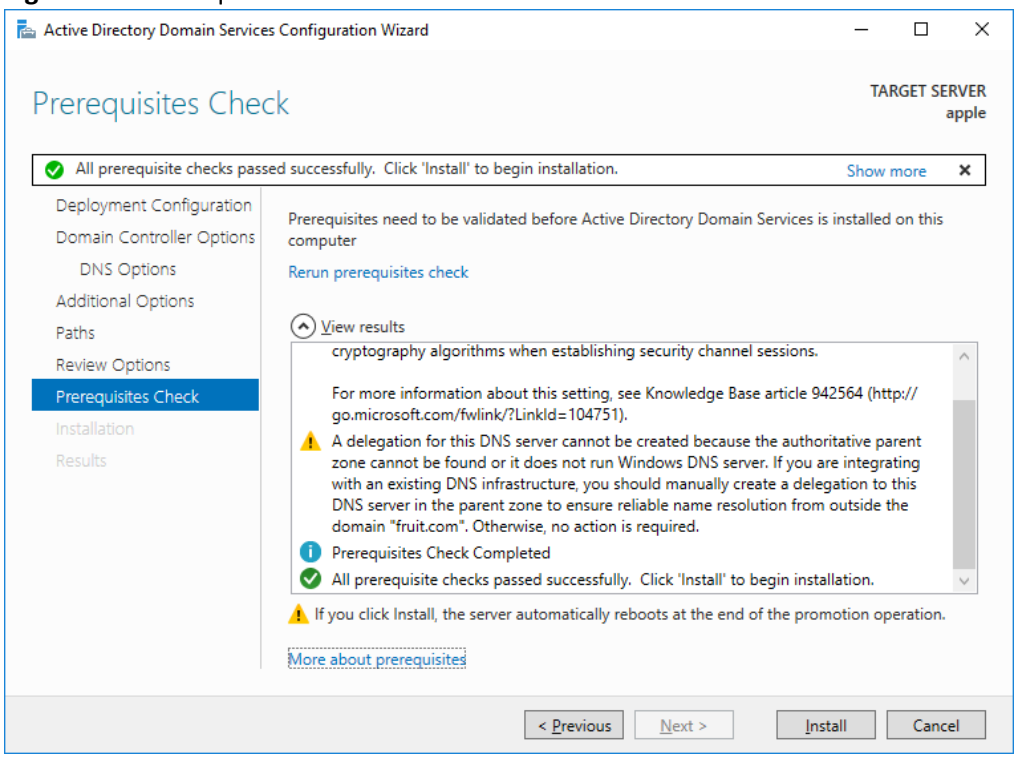
n. The next screen (Figure 17), gives you the opportunity to review your configuration settings. You can also export a PowerShell script to automate future installations. Click, "*View script*" and **save the file**, examine the file. You might even want to try testing an install using the file, it is much quicker to install using the file and PowerShell. Click, ***Next***.

Figure 17 – Review Options



o. 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.

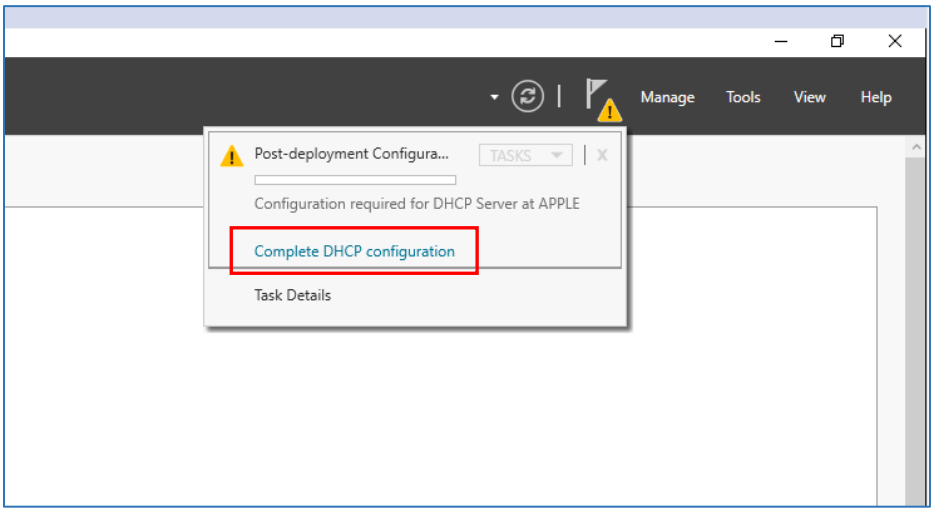
Figure 18 – Prerequisite Check



p. The installation will take several minutes to complete, **be patient!** The system may require a restart, if that happens, you may need to change the Administrator password.

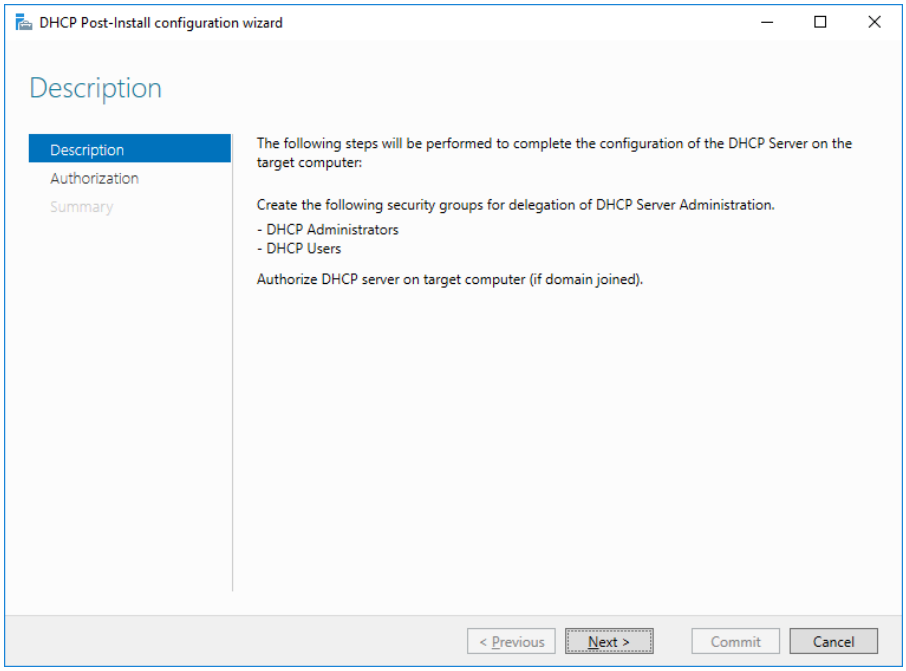
q. Next, you will need to configure the DHCP settings. Click the notifications flag (Figure 19) and select "*Complete DHCP configuration*" to launch the DCHP Post-Install configuration wizard. This will configure who has the ability to manage the DHCP server.

Figure 19 – DHCP Configuration



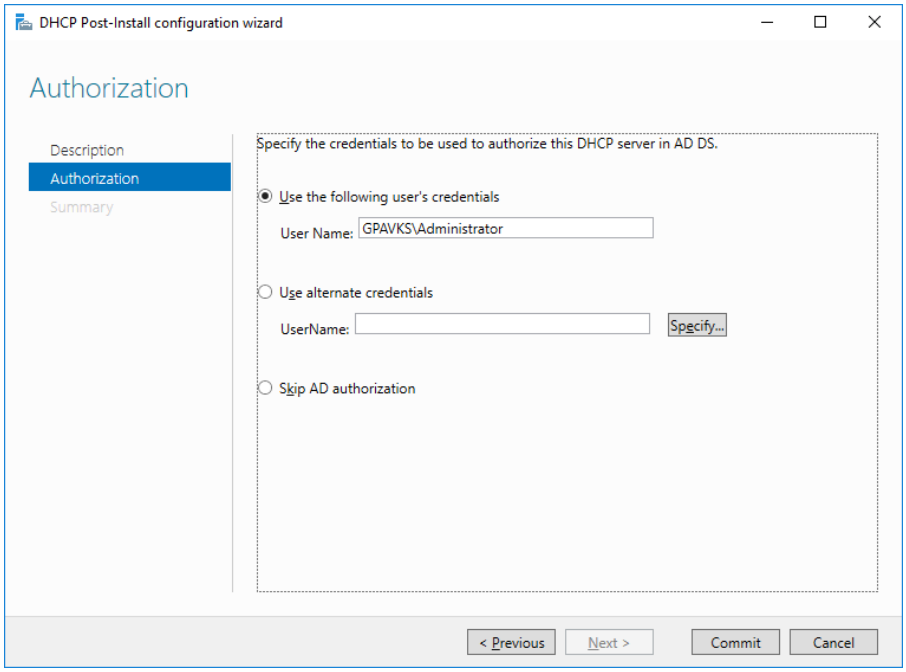
r. The first window to appear will give you information about what you are configuring (Figure 20), read it and click ***Next***.

Figure 20 – DHCP Post-Install Configuration Wizard



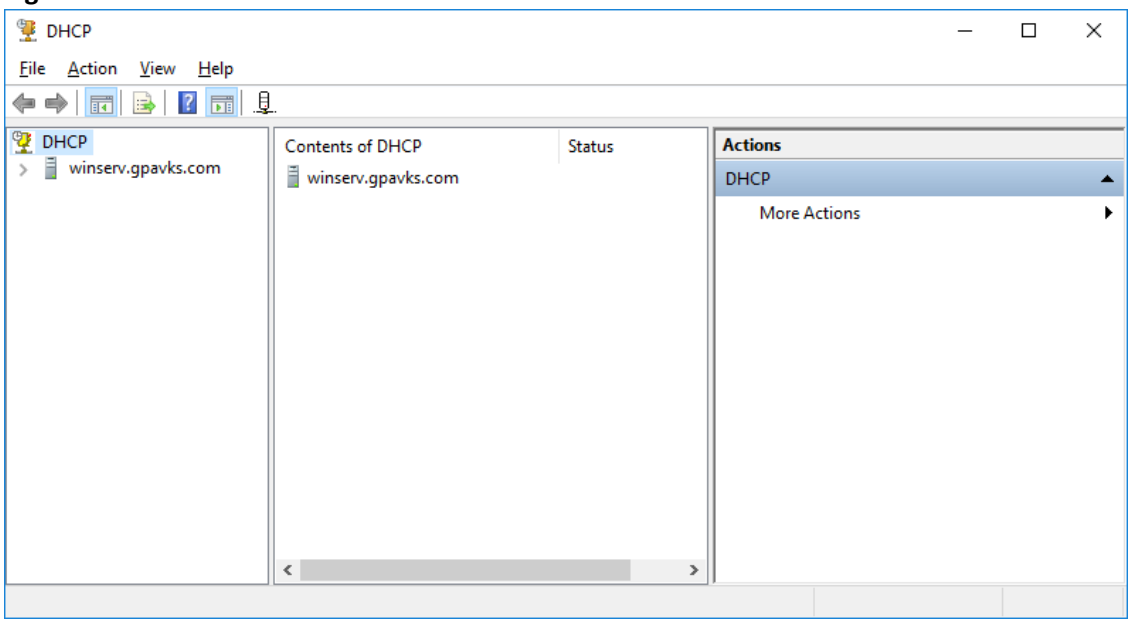
s. The next screen (Figure 21) allows you to select who will be authorized to make changes to the DHCP server, for this lab the Administrator account will be used, **remember this!** Click the ***Commit*** button and then the ***Close*** button on the *Summary* window.

Figure 21 – Authorization



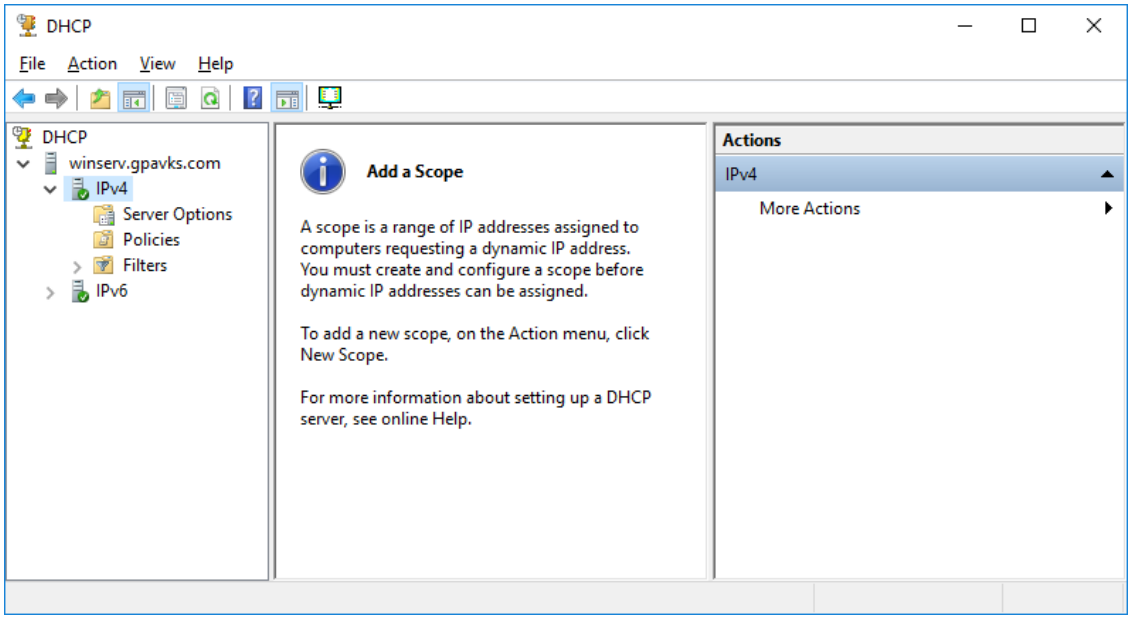
t. To configure the default IP addresses, gateway, and DNS server, perform the following steps. From *Server Manager → Dashboard*, select ***Tools***. From the dropdown menu click ***DHCP***.

Figure 22 – DHCP



u. From the DHCP configuration window (Figure 22) expand the menu for the server to reveal IPv4 (Figure 23).

Figure 23 – Add Scope



v. 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

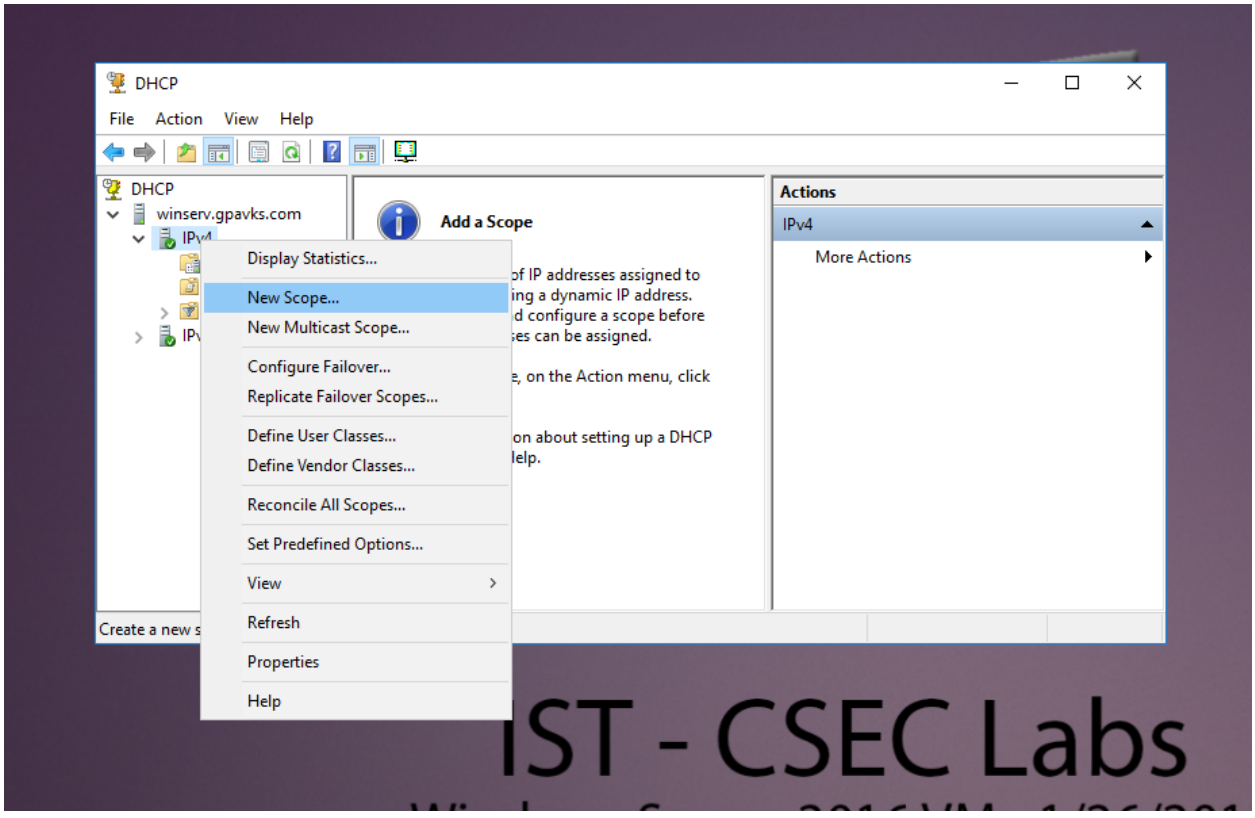
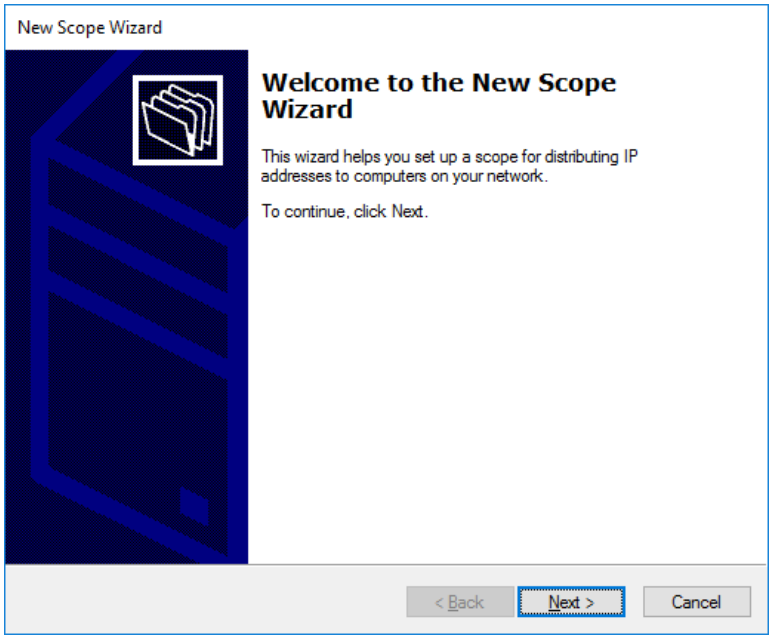
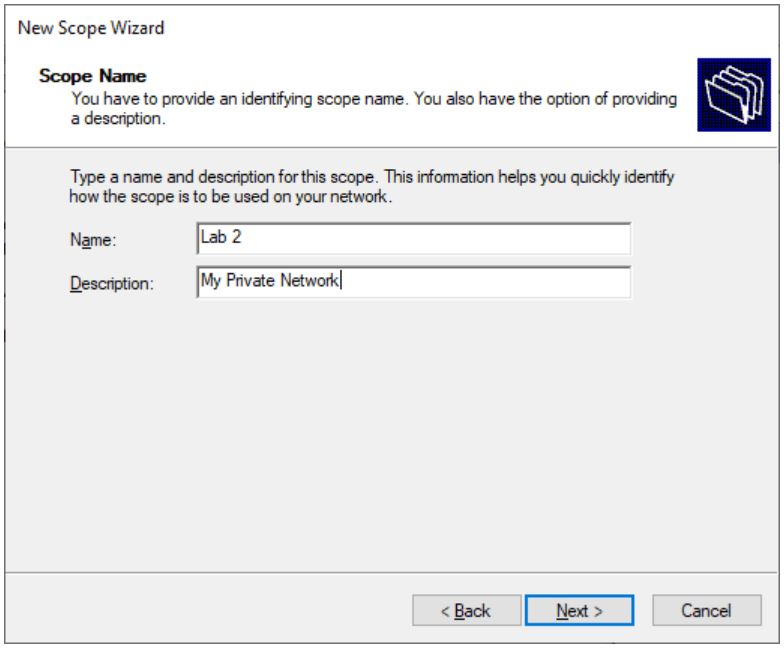


Figure 25 – New Scope Wizard



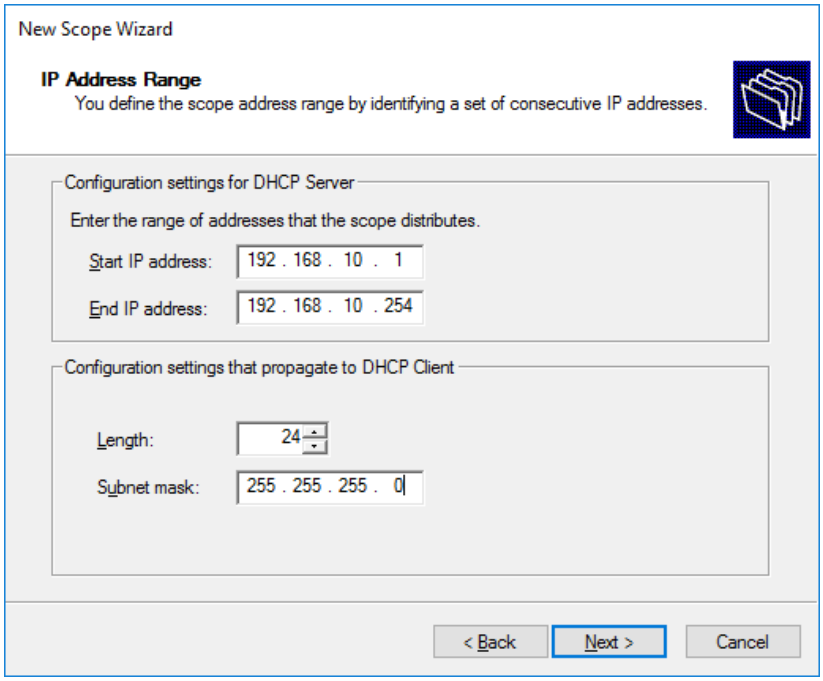
w. On the next window (Figure 26) you may enter a name and description. Click, ***Next***.

Figure 26 – Scope Name/Description



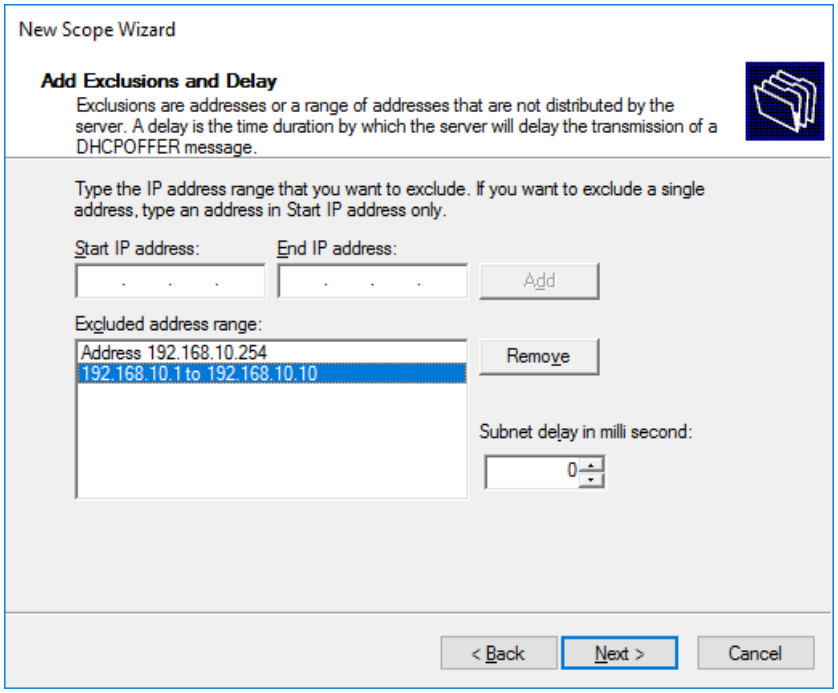
x. Next, define the range of IP addresses that will be available to assign to devices. (Figure 27). Be sure to include the subnet mask and click ***Next***. Again, based on what you did in *Introduction to Routing and Switching* you should have a fundamental understanding of IP addressing and masks.

Figure 27 – IP Address Range



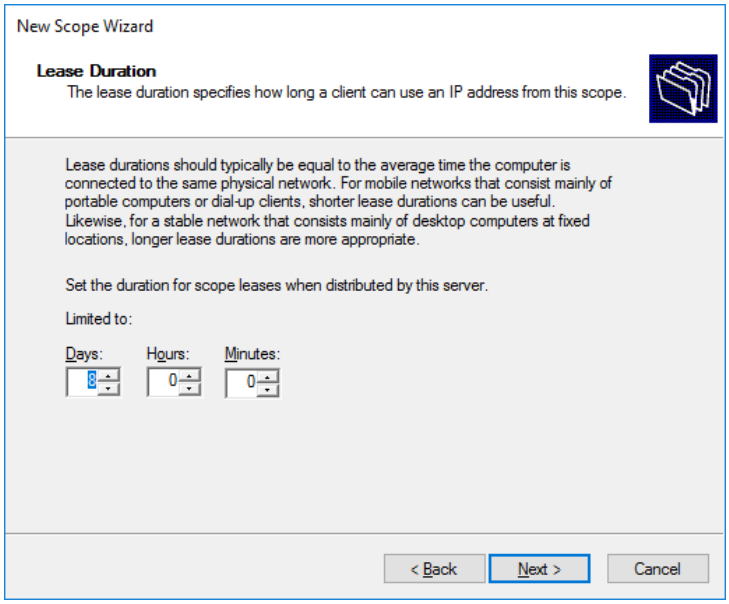
y. On the next window, configure two exclusions, one for the gateway, and another for servers. Exclude the static IP assigned to the default gateway (the pfSense LAN interface). Then, set aside a range of addresses to be assigned to servers throughout the semester, five is sufficient. Referring to the 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



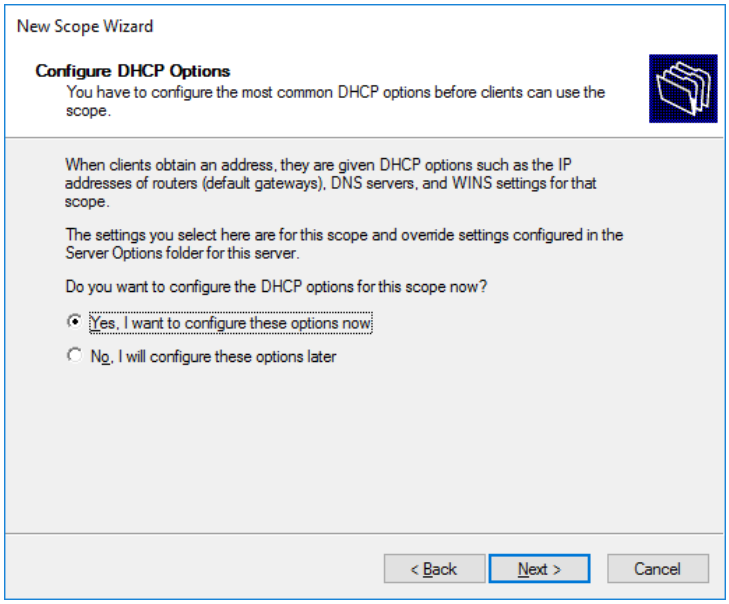
z. Since lab occurs once a week the default setting (8 Days) for the lease time is sufficient (Figure 29). Click, ***Next***.

Figure 29 – Lease Times



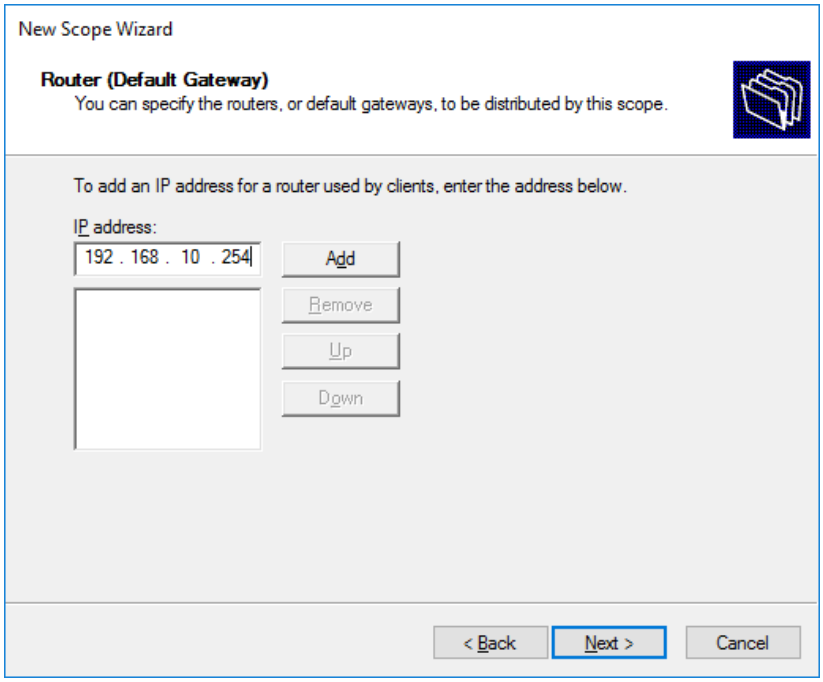
aa. Next, configure the default gateway, and DNS servers by selecting "*Yes. I want to configure these options now*" (Figure 30) and click ***Next***.

Figure 30 – Configure DHCP Options



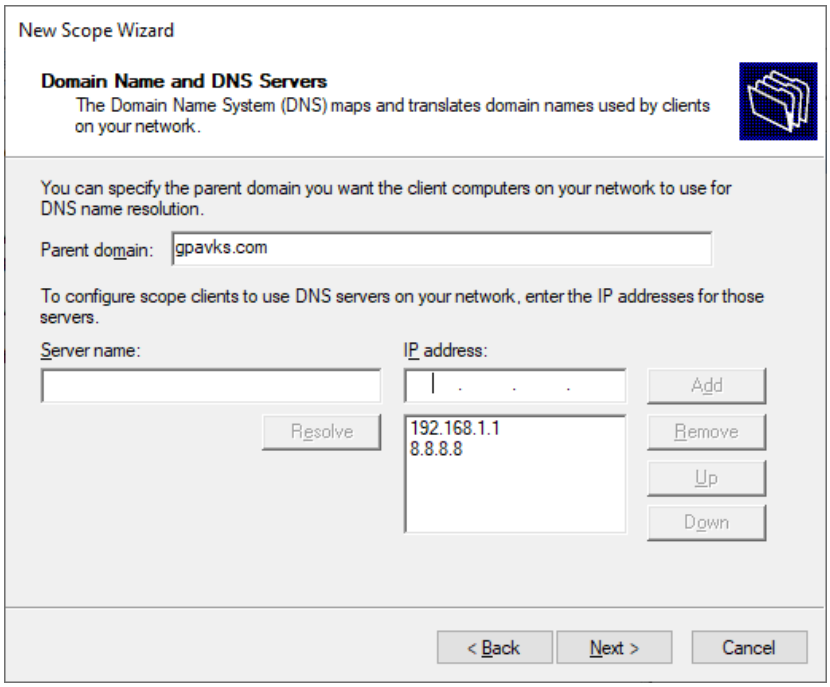
bb. On the next window (Figure 31) enter the default gateway (the LAN interface for pfSense) for your network and click ***Add*** and then ***Next***.

Figure 31 - Configure Default Gateway



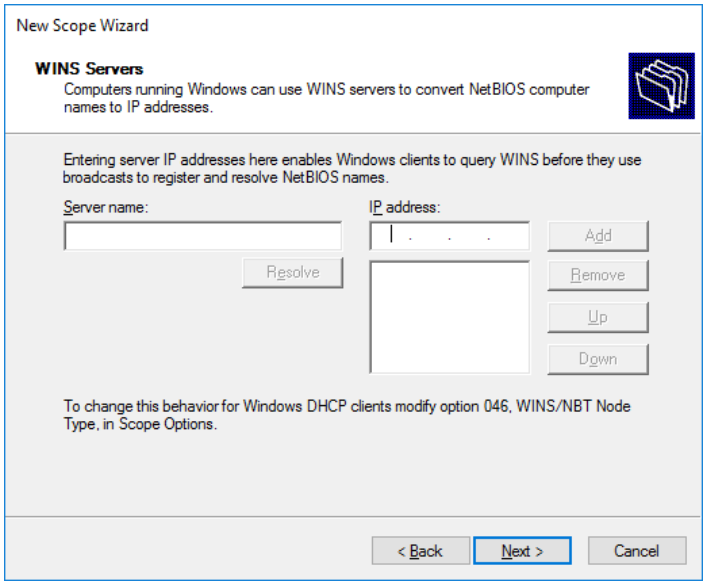
cc. On the next screen (Figure 32), by default, the servers IP address will already be listed as the address for the DNS server, this is what we want. However, using Windows Server will only resolve addresses local to our domain. To resolve addresses in the public realm assign a public server for the secondary DNS, for example 8.8.8.8. Click, ***Next***.

Figure 32 – Domain Name and DNS Servers



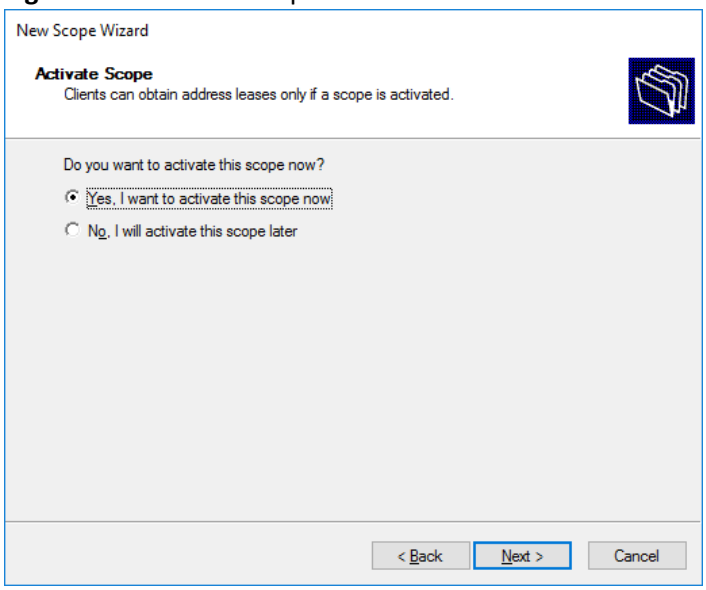
dd. We do not need to configure anything for the Windows Internet Naming Servers, or WINS (Figure 33), click ***Next***. If you're curious, the option is there for backward compatibility with legacy Windows environments.

Figure 33 – WINS Servers



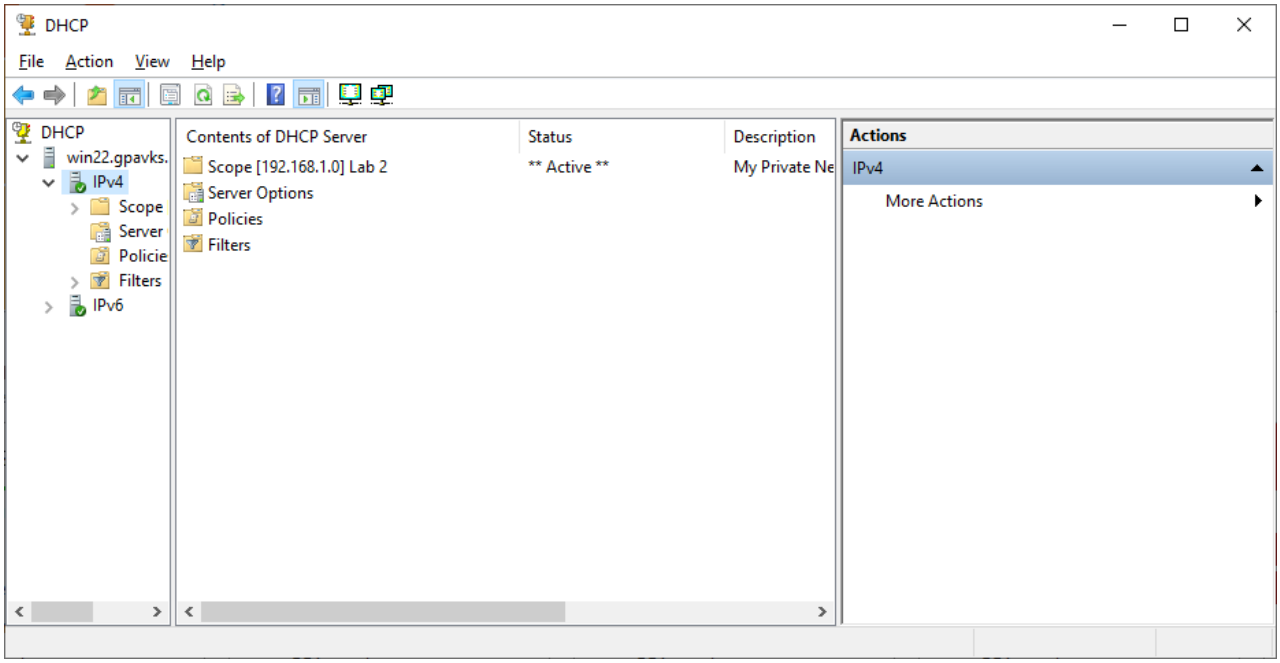
ee. On the next window (Figure 34) activate the scope by selecting the "*Yes. I want to activate this scope now*," radio button and clicking ***Next***.

Figure 34 – Activate Scope



ff. Complete the configuration by clicking ***Finish.*** Close out of the installer and you should see that the scope is now active. (Figure 35).

Figure 35 – Scope Active



In your report, please include the following two screenshots:

Server Information Screenshot:

- Open PowerShell and log in as an Administrator.
- Use the command **`date; Get-ADDomain`** to display the server information. This will also include the date in the output.
- Refer to Figure 36a for an example of the expected output.

DHCP Server Information Screenshot:

- In the same PowerShell session, execute the commands **`date; Get-DhcpServerInDC`** and **`date; Get-DhcpServerv4Scope`**.
- These commands will provide the DHCP server and scope information, respectively, along with the dates.
- See Figure 36b for examples of what these outputs should look like.
- Remember to include the `date` command before each PowerShell command to ensure the date is displayed in your screenshots.

Figure 36a – AD and DHCP Server Information Sample Screenshots

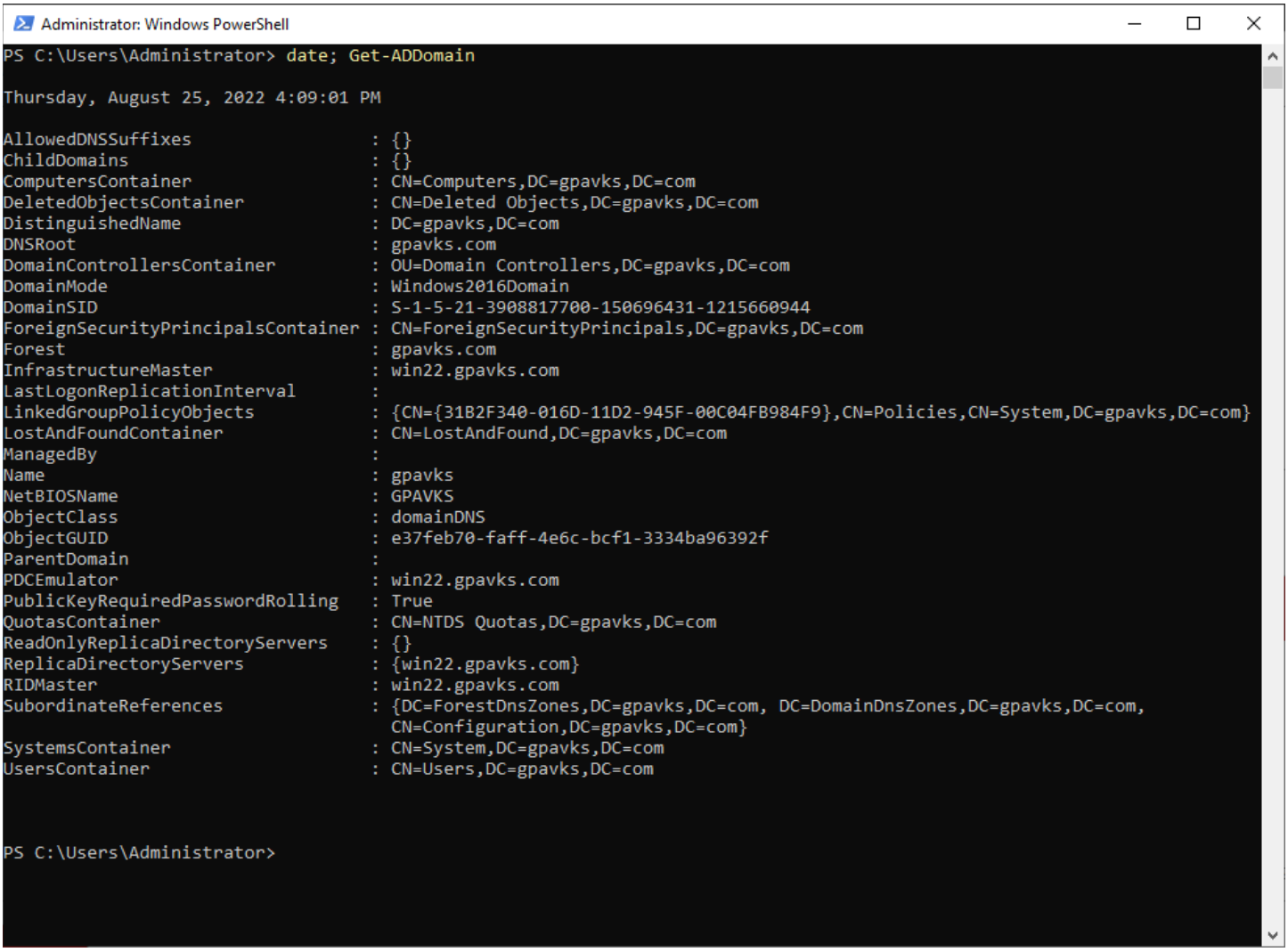
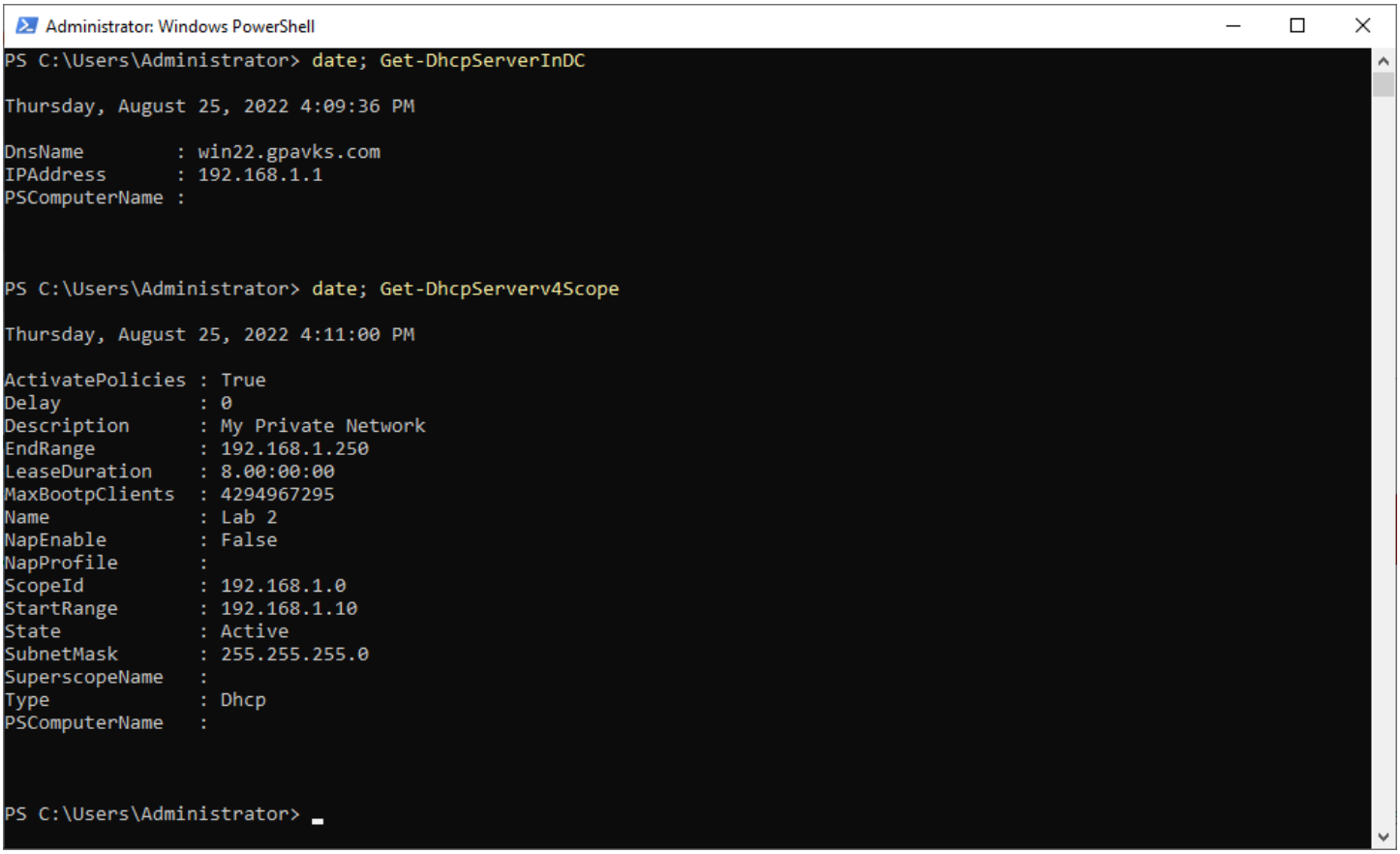


Figure 36b – AD and DHCP Server Information Sample Screenshots

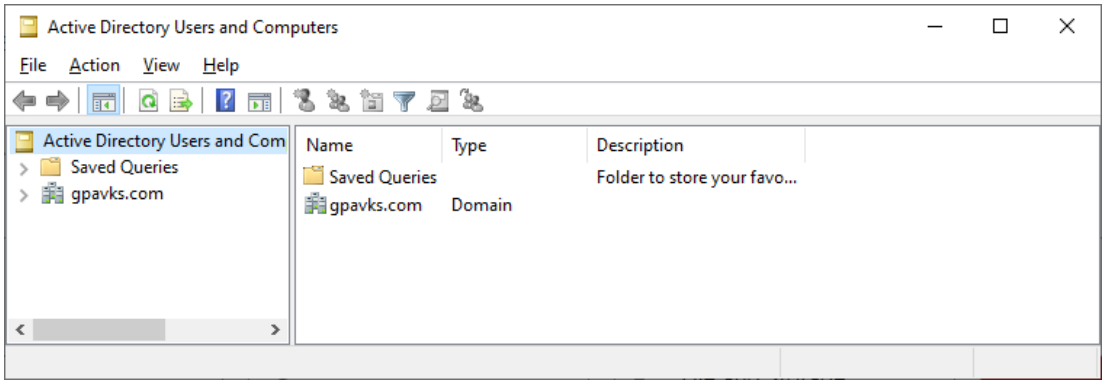


Activity 2 – Create a User Account

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, Samba, or Winbind for a domain controller. But for this activity, you will be authenticating a user from both the Linux and Windows clients using Windows Active Directory.

a. On Windows Server 2025, 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)



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

Figure 38 – Create a New User

c. Create the *New Object – User*, and referring to Figure 39, enter the users first, last, and logon name. Again, the user can be anyone you want, you do not need to follow the screenshot. Generally, login names are the user first initial followed by their surname.

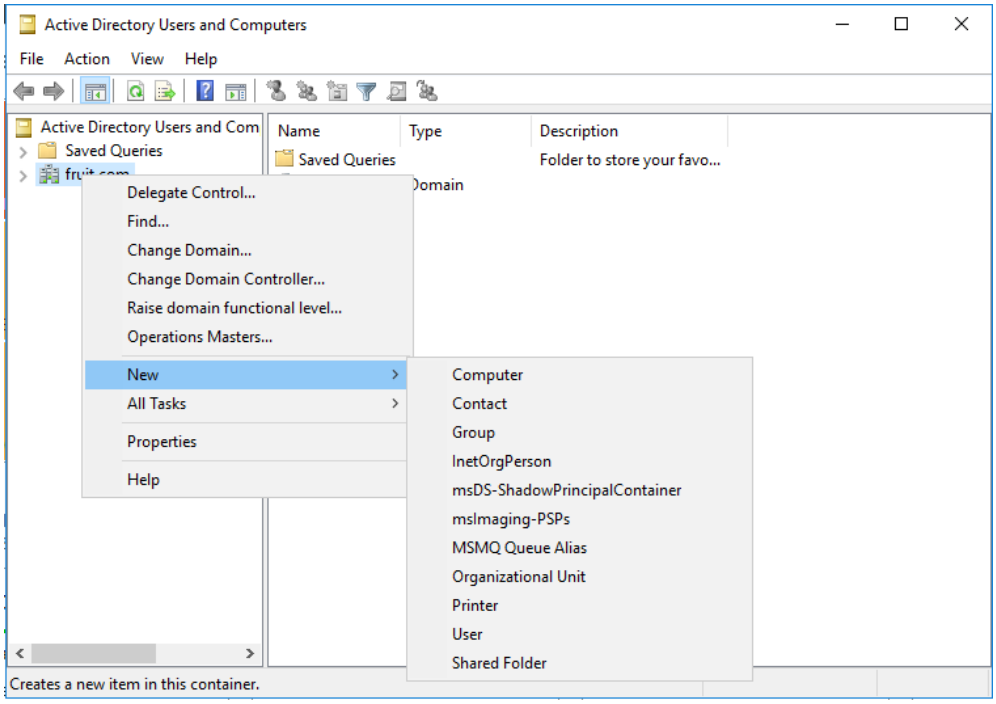
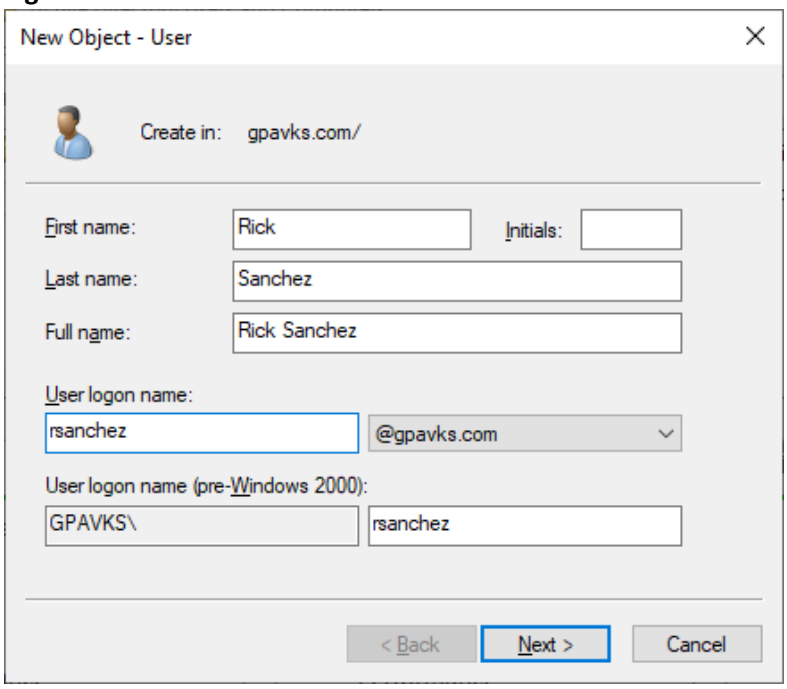
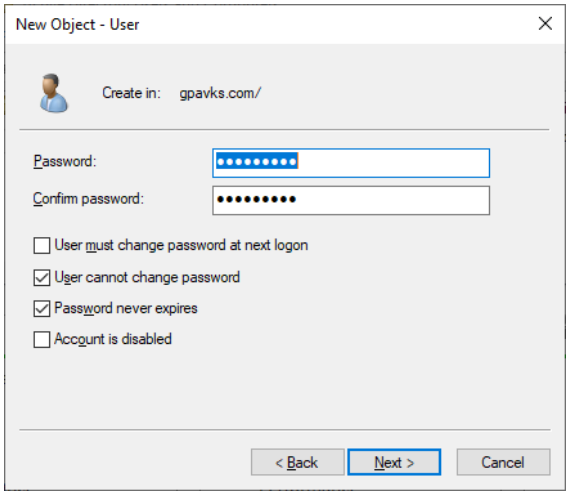


Figure 39 – New User Creation



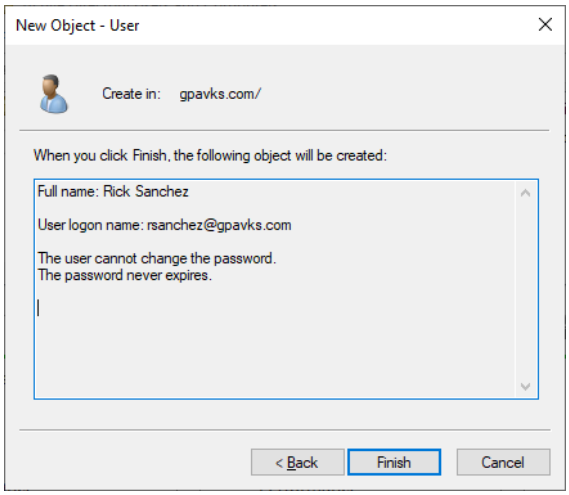
d. Enter a password for the newly created user and uncheck "*User must change password at next logon*", check the boxes for "*User cannot change password*" and "*Password never expires*", click ***Next*** (Figure 40).

Figure 40 – Password Configuration



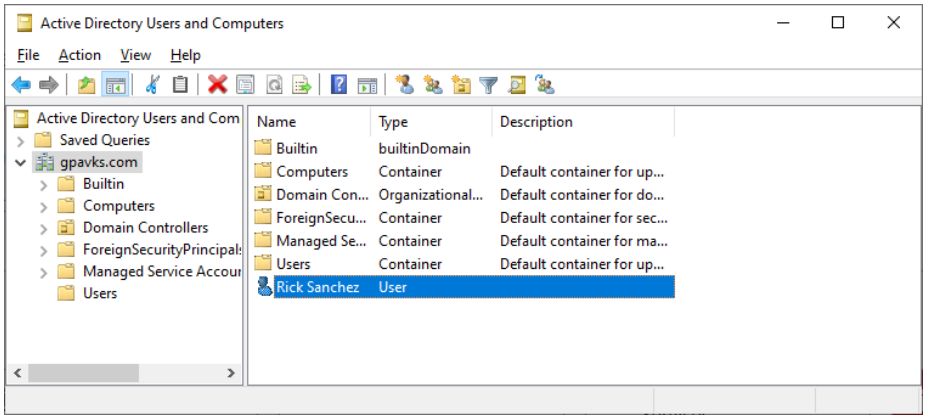
e. The next window, Figure 41, provides a summary of the user information, click ***Finish***.

Figure 41 – User Creation Summary Window



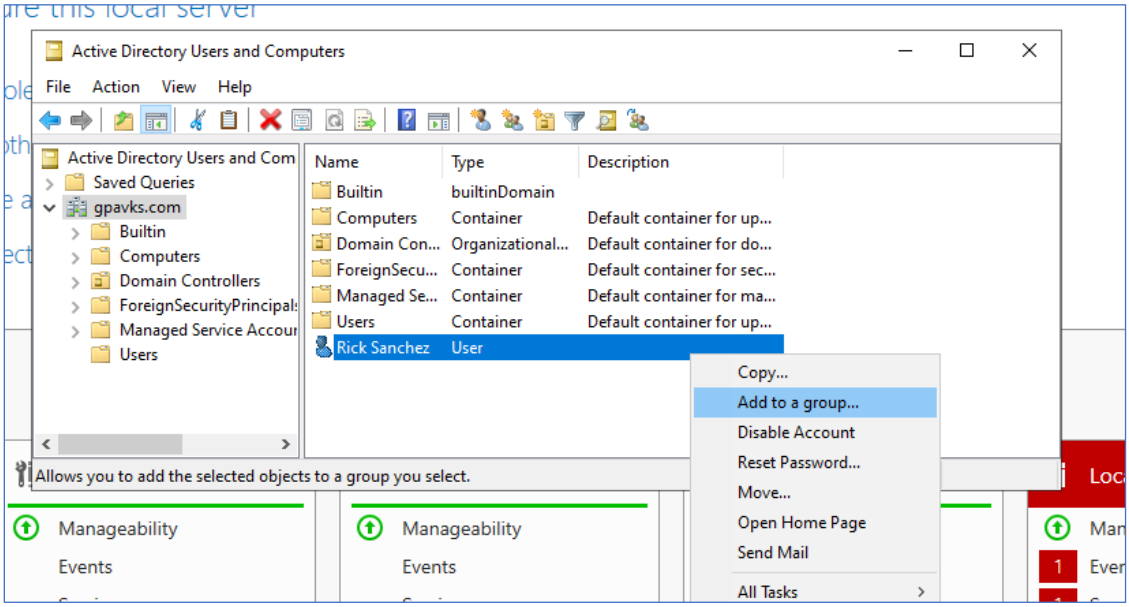
f. The user will appear in the domain (Figure 42).

Figure 42 – Created User in the domain



g. 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



h. 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

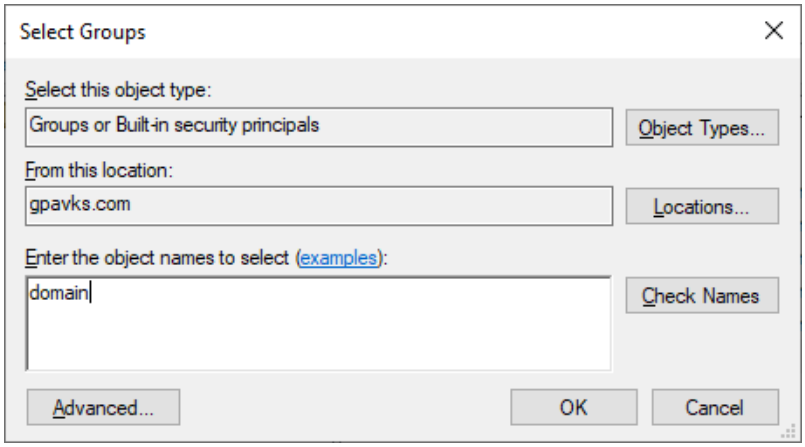


Figure 45 – Matching Names

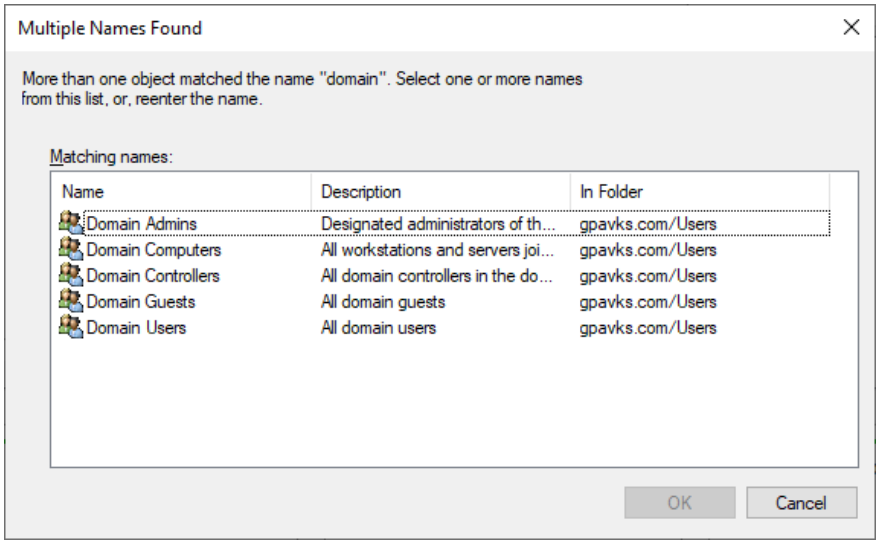
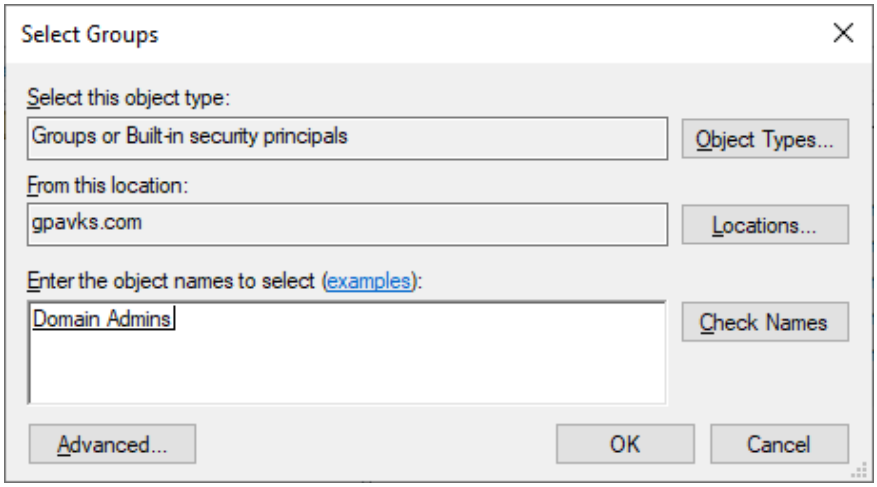
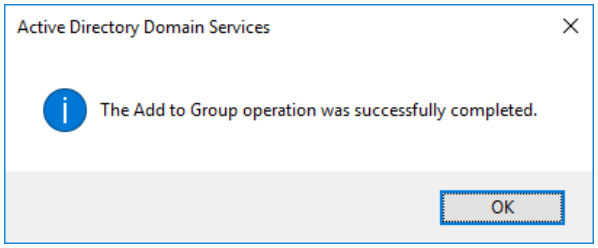


Figure 46 – Select Group



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

Figure 47 – User Successfully Added Confirmation



Activity 3 – Joining User to the Windows Domain

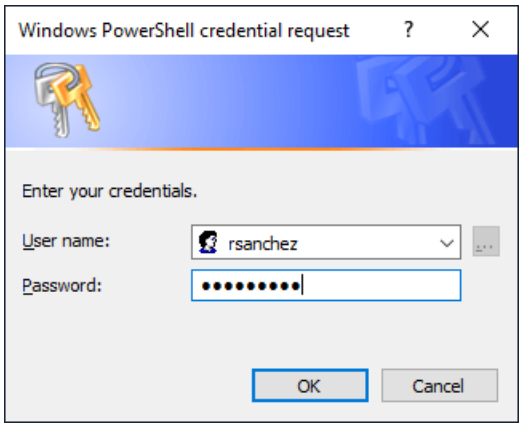
For this activity, you will join the user you created in the previous activity to the domain by remotely authenticating to the Active Directory server from the Linux and Windows workstations.

a. Power on the Windows and Linux clients. Again, make sure to attach the virtual NICs to the LAN Segment.
b. Change the NIC settings on the clients to receive their respective IPv4 network **configurations via DHCP**. Remember they were configured statically in Lab 1. Verify that the settings are configured for DHCP using the **`ipconfig /all`** command.
c. On Windows 11, open PowerShell and run as Administrator.
d. Enter the following command, using your domain suffix.

```
Add-Computer –DomainName gpavks.com –Credential (Get-Credential)
```

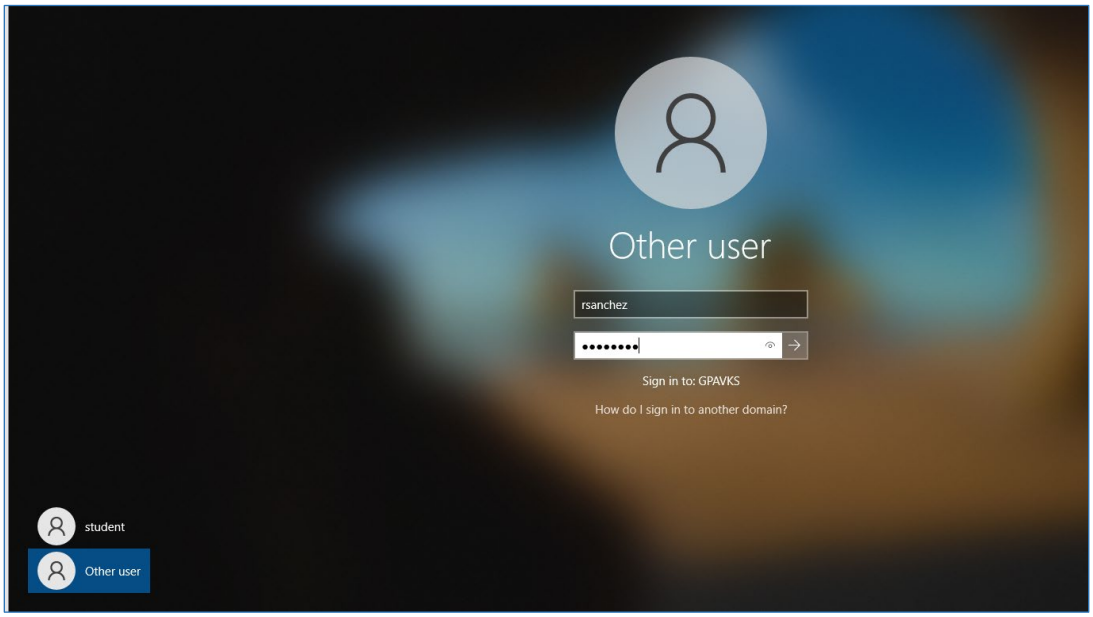
e. When prompted enter the test users' user name and password, Figure 48.

Figure 48 – Windows 11 Credential Request



f. Click OK. You will be prompted to restart the system.
g. Once Windows restarts, you will need to select ***Other User*** to log into the domain. Notice too that it tells you the domain you are signing into, in this example it is GPAVKS.

Figure 49 – Logging into Windows 11

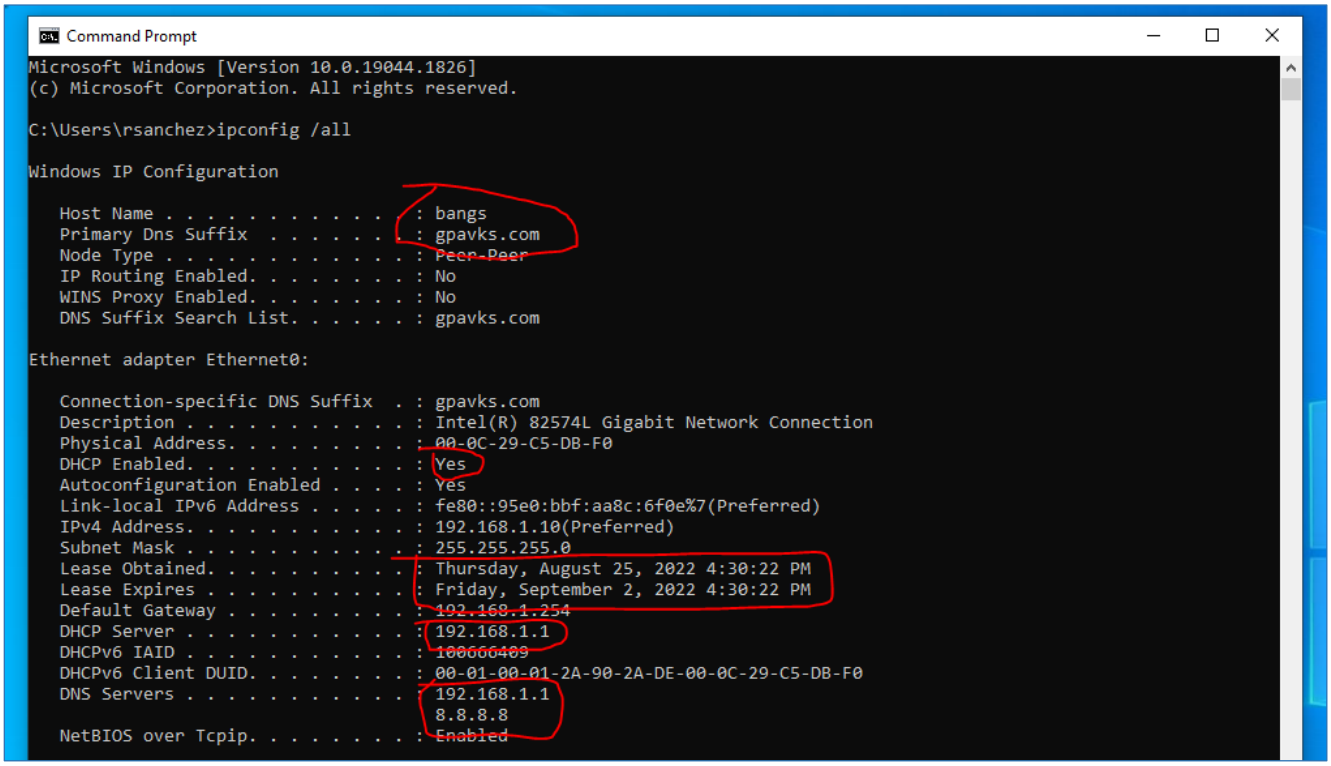


For your report, please include a screenshot showing the Windows 11 IP Configuration and Adapter Settings. This screenshot needs to show that Windows 11 has received its IP address from the Windows server via DHCP. For an example of the expected output, refer to Figure 50.

Ensure the following details are visible and legible:

- Host Name
- Primary DNS Suffix
- DHCP enabled (Yes)
- DHCP lease information
- The DHCP server address
- The DNS server address

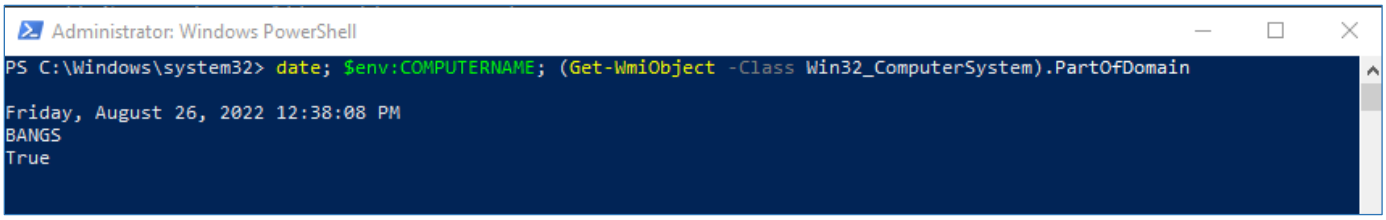
Figure 50 – Sample Screenshot Showing Network Configuration Settings for Windows 10



A second screenshot showing that the Windows 11 client is a member of the domain (Figure 51). Use the following command (this is all one line).

```
PS C:\Windows\system32> date; $env:COMPUTERNAME; (Get-WmiObject -Class
Win32_ComputerSystem).PartOfDomain
```

Figure 51 –Windows 11 Domain Membership Verified



h. On the Linux VM, log in as "*student*", using the default password "*student*". Optionally, for convenience, you may want to log in as "*root*".

i. Open a terminal, go to Activities → 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".

j. As root, update the Rocky VM by typing the following command. **Updating is important!**

```
dnf -y update
```

k. The update may take some time, so be patient.

l. Check the Rocky **documentation** to see what packages need to be installed.

https://docs.rockylinux.org/guides/security/authentication/active_directory_authentication/

m. Referring to Figure 53, using the **`dnf list`** command and by piping grep, we can check so see if the system has the required installed packages. Remember, the **`dnf`** command replaces **`yum`** in Rocky, although you can still use the **`yum`** command as it is backward compatible. Refer to the **`dnf cheatsheet`** in myCourses for more information on the command and the associative arguments.

Figure 53 – Example Search for adcli package

a. If any packages are missing, use `dnf` to install them.

b. You may also want to check to verify that the services are running. The following command checks the status of realmd.

```
systemctl status realmd
```

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

```
systemctl start realmd
```

d. To make sure the service starts when the system boots, use the following command.

```
systemctl enable realmd
```

e. If you need more information on how to start, stop, and enable services, refer to the **man pages** for the `systemctl` command.

f. 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.

```
realm join --user=rsanchez gpavks.com
```

Or

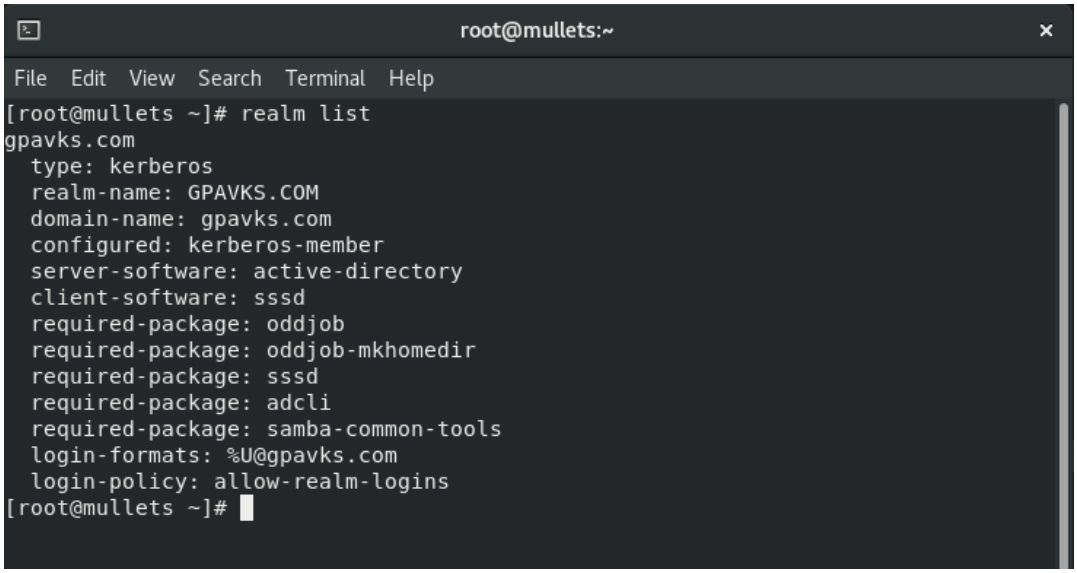
```
realm join -U <user name> <domain name>
```

g. To verify that you are join to the domain, type the following command.

```
realm list
```

h. The output will look similar to Figure 54. If the realm is not listed check to make sure the correct packages are installed and running.

Figure 54 – Realm List Output Sample



i. Next log out of the system and login as the Active Directory user, using the User Principal Name. For example, rsanchez@gpavks.com and then the password.

To validate completion of this activity for your lab report, you are required to include a single comprehensive screenshot. This screenshot must visibly display the following key pieces of information:

Comprehensive Screenshot Requirements:

- The current date.
- The Active Directory user currently logged in.
- The realm details.
- The VM's hostname.

Commands to Execute:

To gather the necessary information, execute the following commands in your VM's terminal:

- `date`
- `whoami`
- `hostname`
- `realm list --name-only`

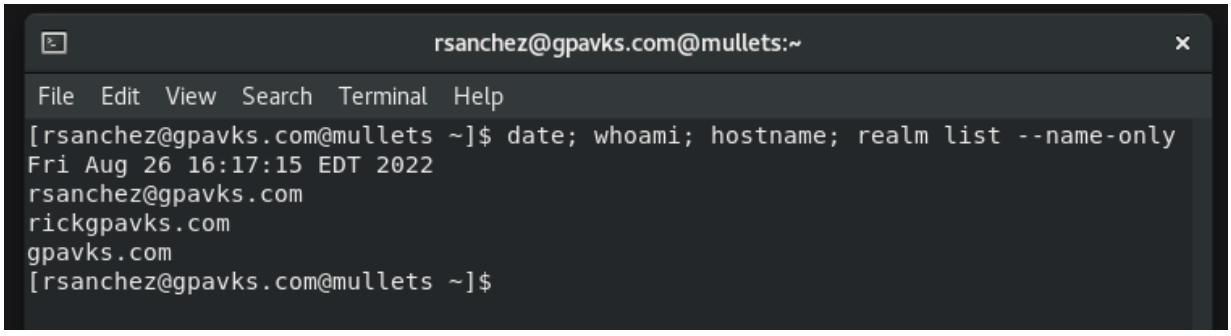
Arrange the terminal window so that the output of all these commands is visible in one screenshot.

Reference for Expected Output:

For guidance on how this screenshot should look, please refer to Figure 55.

Ensure that all the required information is legible in the screenshot to successfully validate your completion of this activity.

Figure 55 – User Login Verification

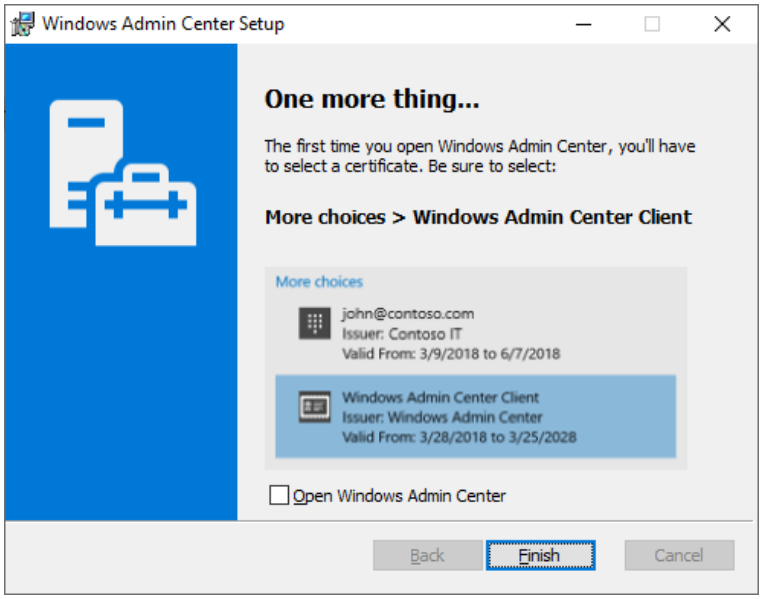


Activity 4 – Remote Management

To remotely access the Active Directory Server, this lab will use two methods. In most enterprise environments, it is unlikely that you will have physical access to the server and need to remote in from another device. In Linux, the Secure Shell is the preferred method. We have several options on Windows, but this lab will use Windows Admin Center and PowerShell. The First task is to install Windows Administrative Center on Windows 11 and then use PowerShell. Once remote access is established, the next activity will walk through creating Organizational Units (OUs) and adding more users.

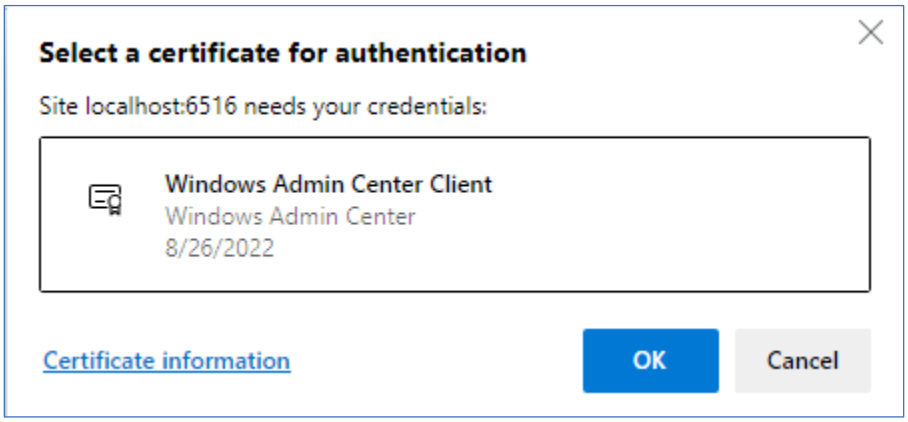
a. Install Windows Admin Center on Windows 11 by downloading it from the following link. You'll have to register and provide some information. Install using the default settings. Check the box to "*Open Windows Admin Center*," Figure 56. And click "*Finish*."

Figure 56 – Open Windows Admin Center



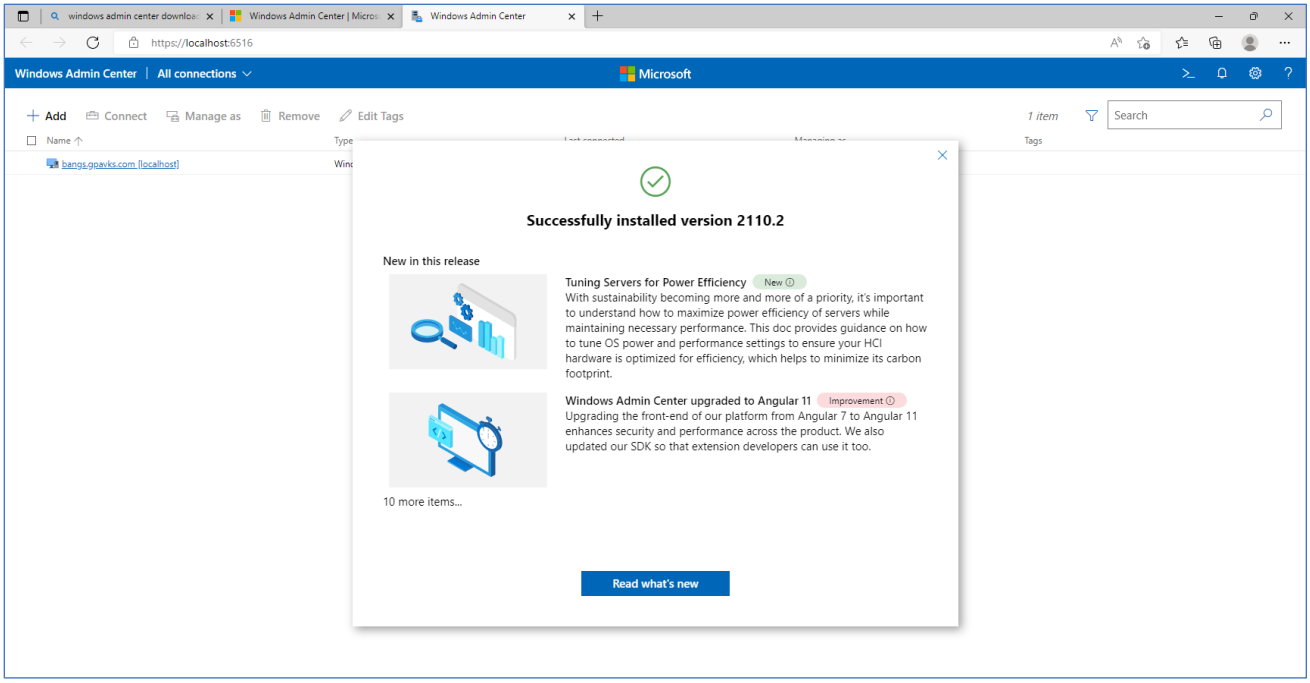
b. Select the certificate (click in the box) and then ***OK*** to accept the certificate for authentication, Figure 57.

Figure 57 – Accept Certificate



c. The following message will appear indicating that the installation was successful, Figure 58.

Figure 58 – Installation Successful

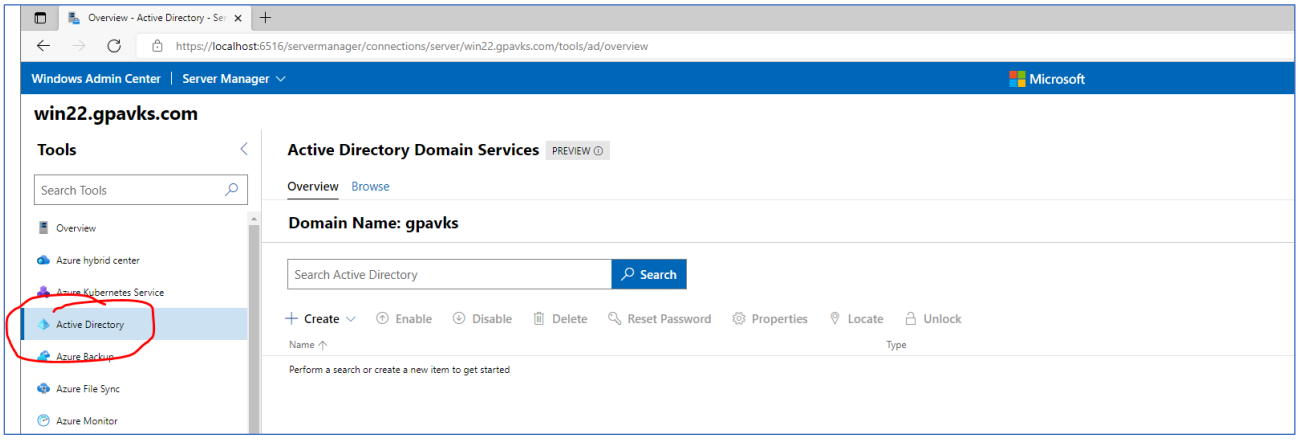


d. If prompted update any required extensions.
e. Next, install the Active Directory extension. To do this, refer to the Microsoft Windows documentation.

https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/using-extensions

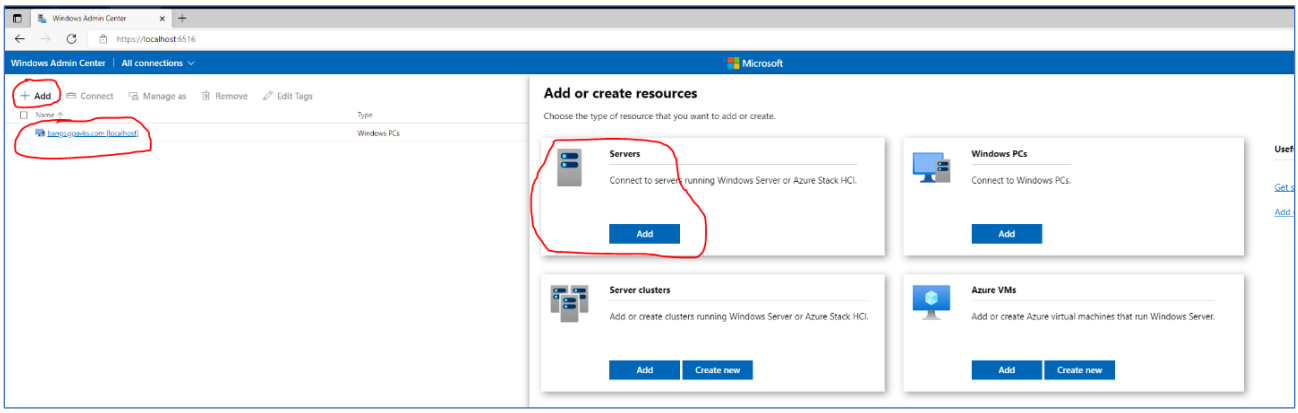
Once it is installed it will appear in the "Tools" column (Figure 59).

Figure 59 – Active Directory Extension



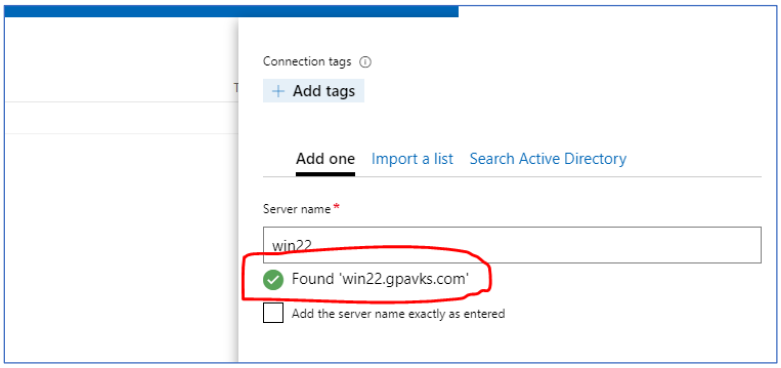
f. Next, connect to the server by clicking +Add button and the Add button in "Servers," Figure 60. Add this point the only device you should see is the Windows 11 client.

Figure 60 – Add the server



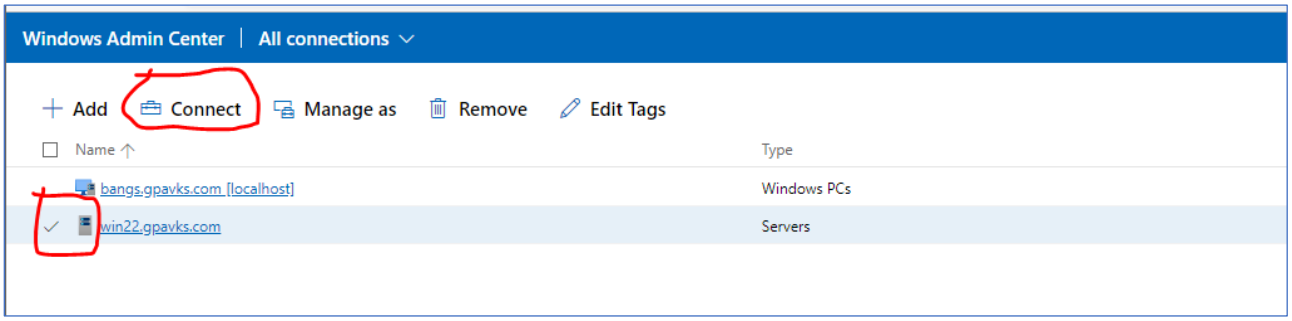
g. Enter the hostname you assigned to Windows Server 2025. Window Administrative Center should find it, if not troubleshoot, network and DNS configurations. Otherwise, you will see a green check and the FQDN of the server, Figure 61.

Figure 61 – Server Found



h. Next, click the "***Add***" button to add the server to Windows Admin Center. It will appear has a link, Figure 62. Check the box and select "***Connect***."

Figure 62 – Windows Features Install

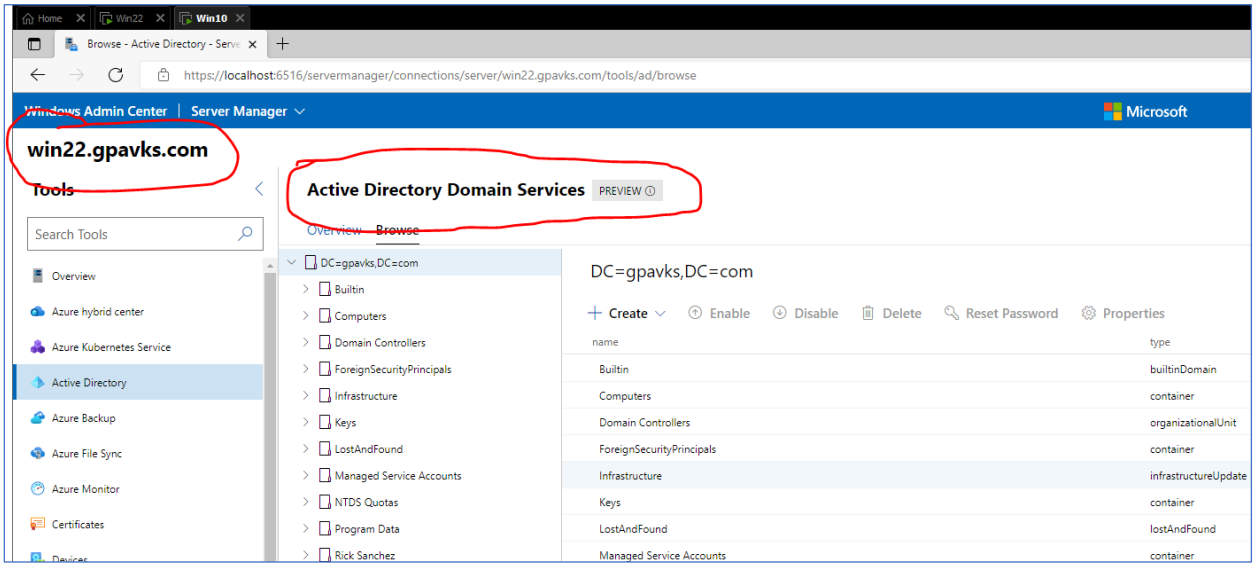


i. Once you have connected to the server, select Active Directory from the Tools, and click on Browse. Take some time to explore other features Microsoft Admin Center offers.

https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/overview

For the report, include a screenshot showing that you have successfully install Windows Admin Center and connected to Active Directory Domain Servers. The screenshot must show the FQDN of the Windows Server and the Active Directory Domain Service Preview, see Figure 63 for reference.

Figure 63 – Sample Screenshot



j. 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 "*win22*."

```
Enter-PSSession -ComputerName win22
```

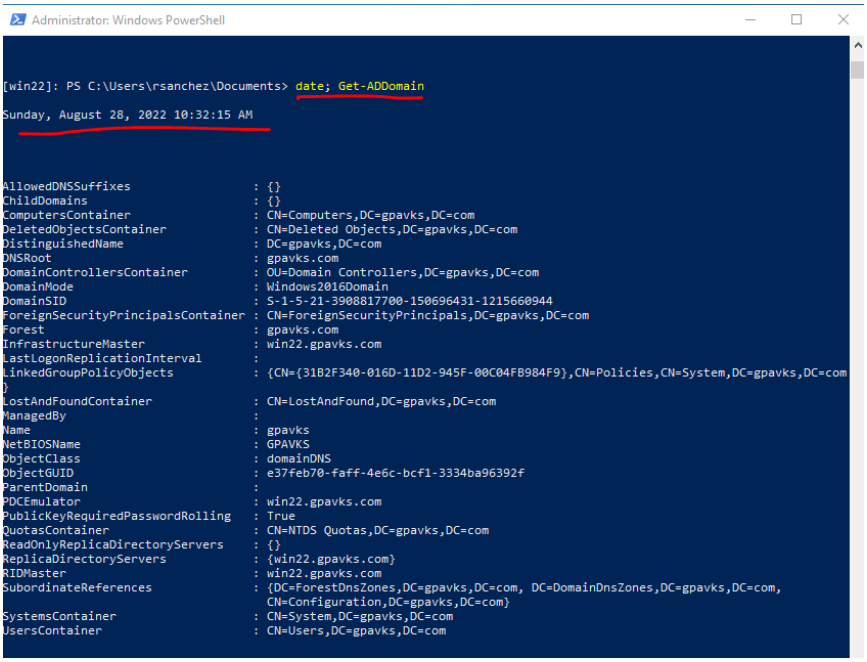
k. We can also use PowerShell to quickly find information about the domain by typing the following command.

```
Get-ADDomain
```

l. Alternatively, you could connect with PowerShell in Administrative Center, in which case you would not need to use the **`Enter-PSSession`** command, since it is automatically done for you behind the scenes.

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

Figure 64 – Sample Screenshot for PowerShell Session and ADDomain Output



Activity 5 – Creating Organizational Units and Adding Users

For this activity, you will use Windows Admin Center from the previous activity to create organizational units and add users to them. Additional tasks will be done remotely using PowerShell.

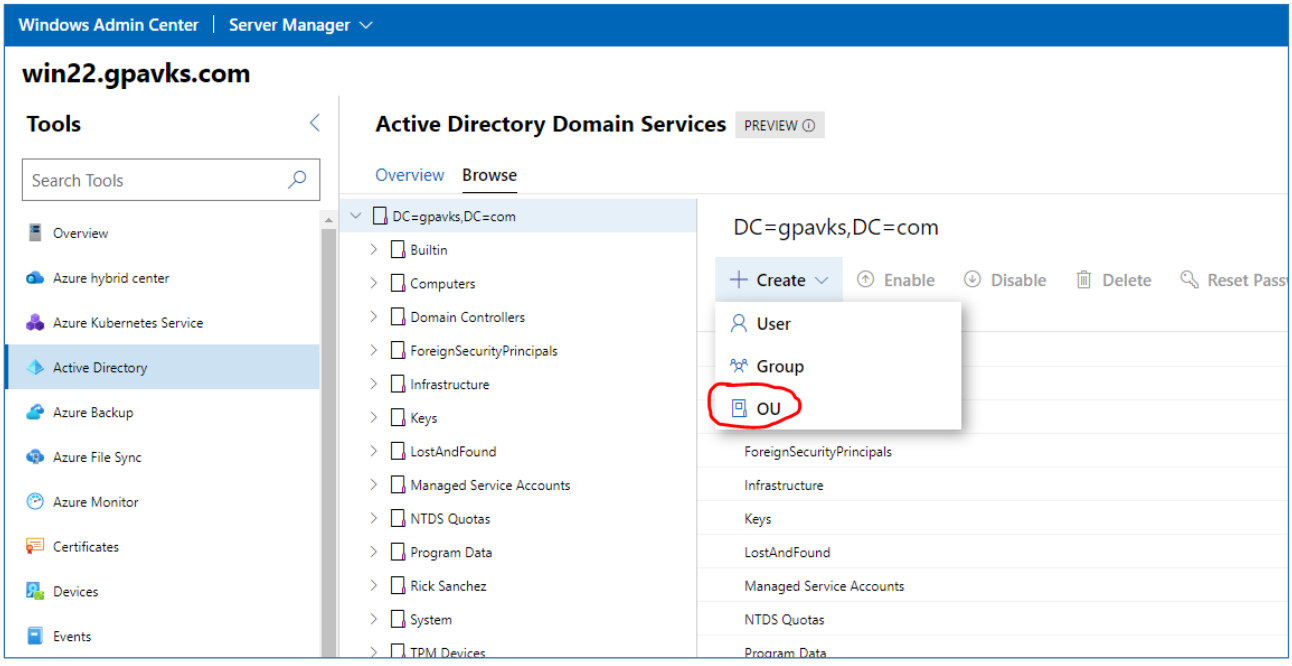
a. Using Windows Admin Center create two organizational units (OUs) and add a minimum of four users to them, you may use the sample information provided in Table 1, or create your own Organizational Unit (OU)and users.

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

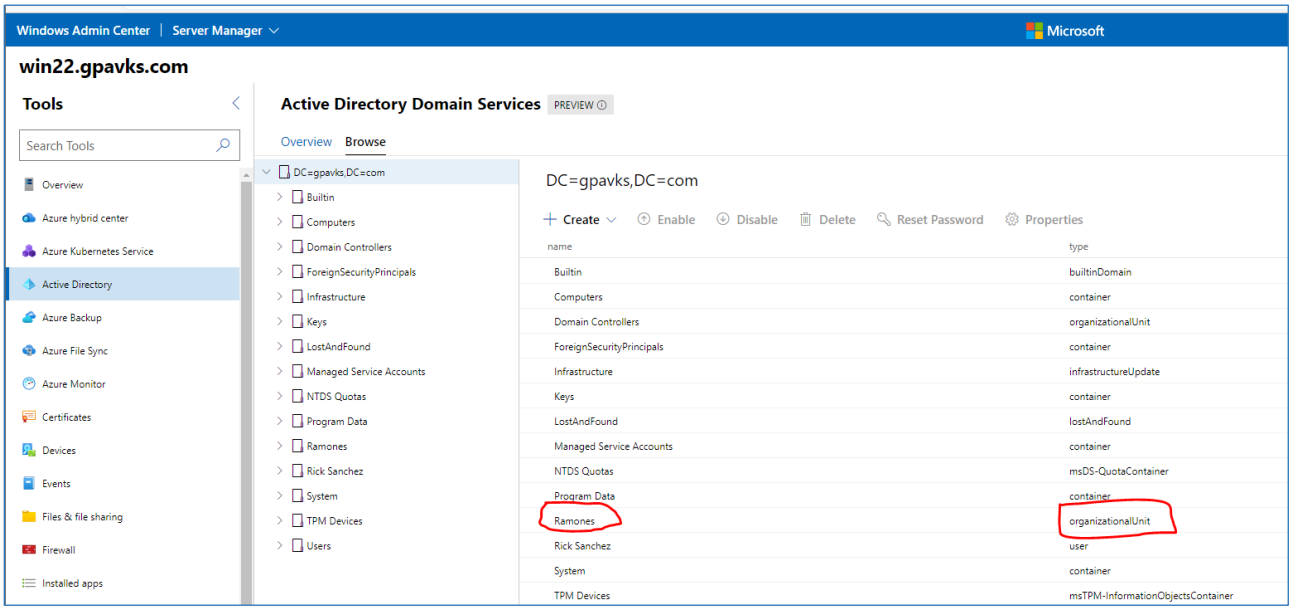
b. Create an organizational unit by clicking ***Create → OU*** (Figure 65). Make sure you are in the domain (i.e., DC=gpavks, DC=com), where ***gpavks*** is the domain in this example.

Figure 65 – Adding an Organizational Unit



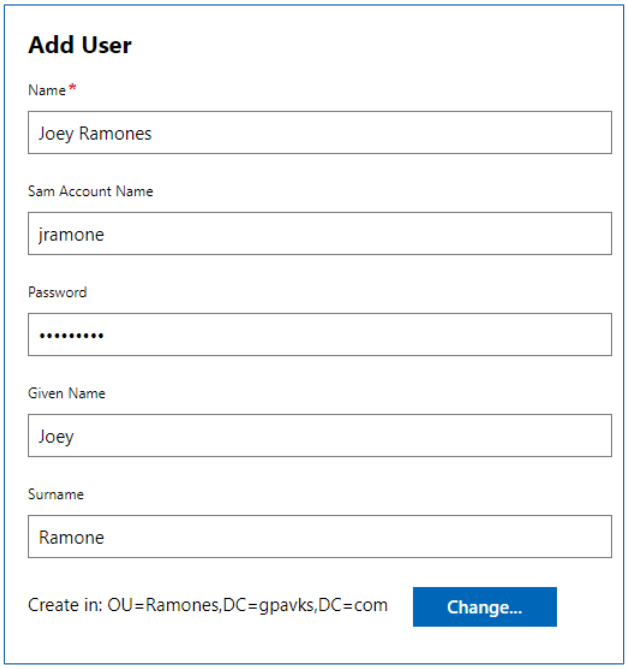
c. To create an organizational unit, enter a name in the *Name* field, optionally you can add information to the description box and click ***Create***. When you have completed this step, the Organizational Unit will appear in the domain in Active Directory (Figure 66). If not try refreshing Admin Center.

Figure 66 – OU listed in domain



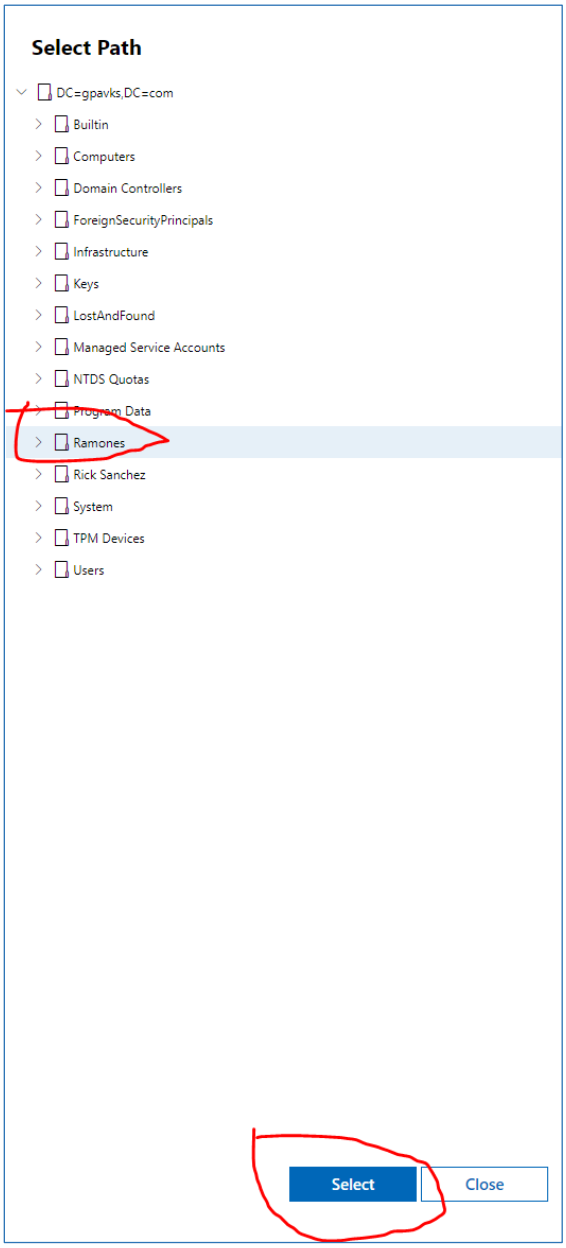
d. To add a user to the Organizational Unit, click the ***Create*** button and then enter the required information (Figure 67).

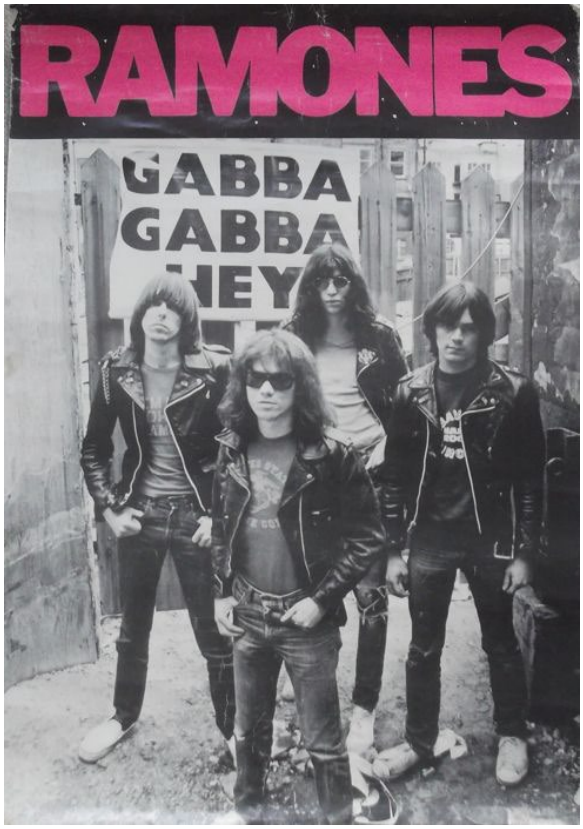
Figure 67 – Adding the User



e. Next add the user to the Organizational Unit by clicking ***Change***, highlighting the OU and hitting ***Select*** (Figure 68).
f. Next, hit ***Create*** to add the user.

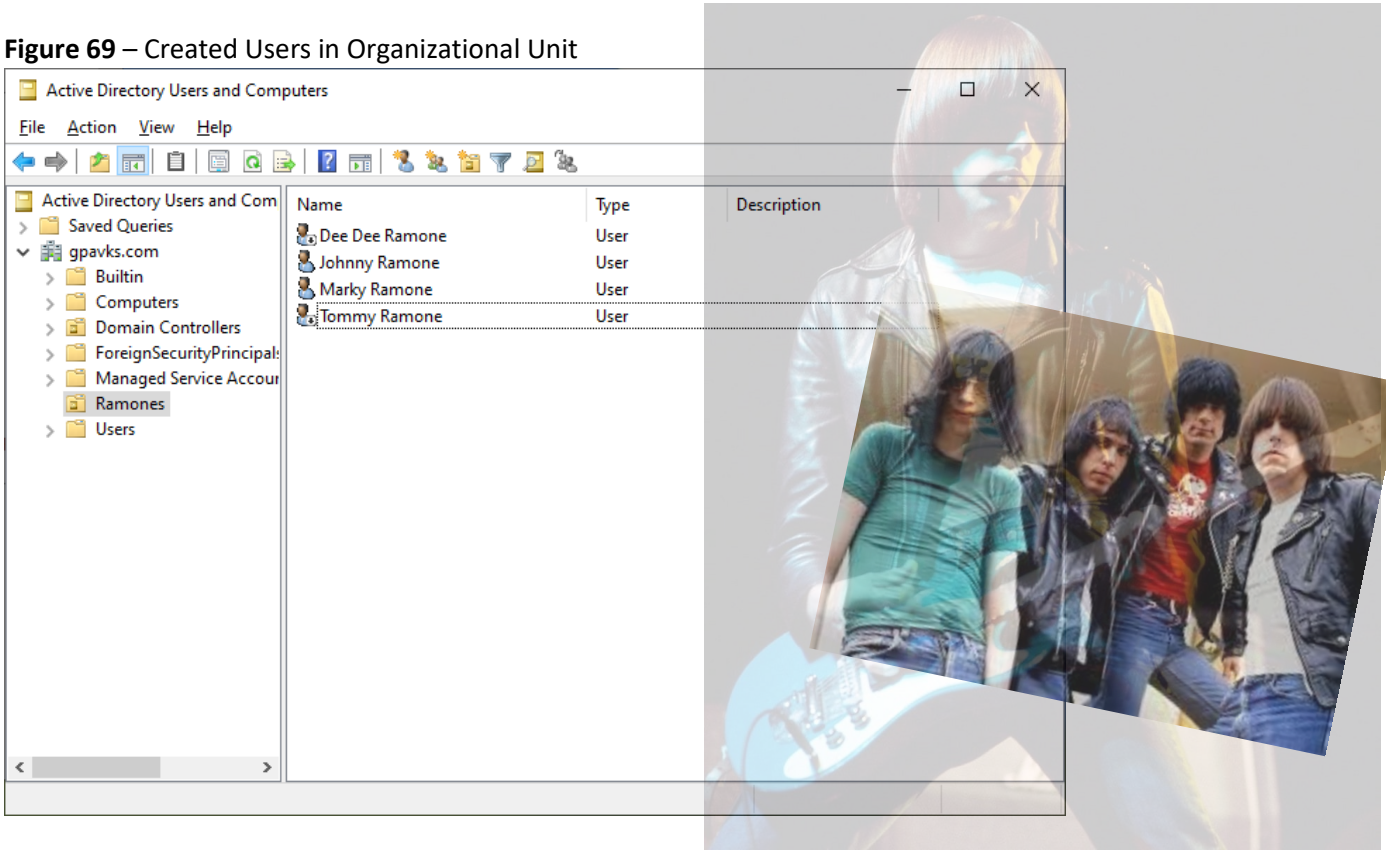
Figure 68 – Adding a User to the Organizational Unit





g. Repeat the process to add the other users to the Organizational Unit. When finished go to Windows Server 2025 and Active Directory Users and Groups (ADUC), to see the users listed in the organizational unit.

Figure 69 – Created Users in Organizational Unit



h. Use PowerShell to create a second Organizational Unit in your domain with four new accounts. You may use the information in Table 2, or create an organizational unit and associated users unique to your domain.

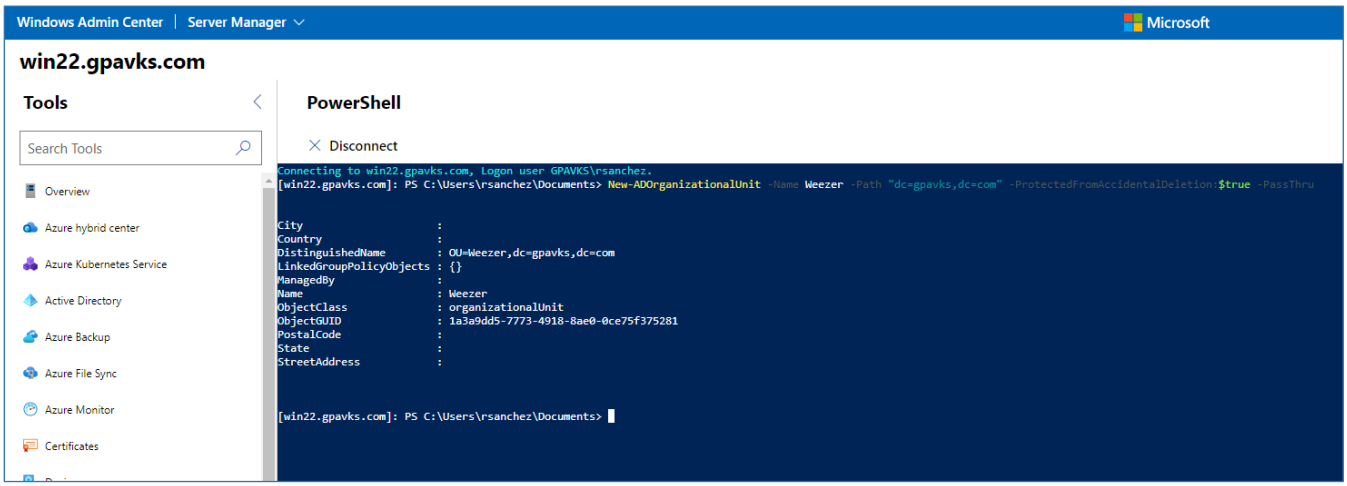
Table 2 – Users in the **Weezer** Organizational Unit

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

i. 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 70.

```
New-ADOrganizationalUnit -Name Weezer -Path "dc=gpavks,dc=com" -
ProtectedFromAccidentalDeletion:$true -PassThru
```

Figure 70 – Organizational Unit Creation Using PowerShell



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

```
New-ADuser –Name “Patrick Wilson” –GivenName Patrick –Surname Wilson –
UserPrincipalName “pwilson@gpavks.com” –SamAccountName pwilson –Path
“ou=weezer,dc=gpavks,dc=com”
```

k. Repeat the command to add additional users to the Organizational Unit.

l. 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.

```
Set-ADUser –Identity “CN=Patrick Wilson,OU=weezer,DC=GPAVKS,DC=COM” –
OfficePhone “5624”
```

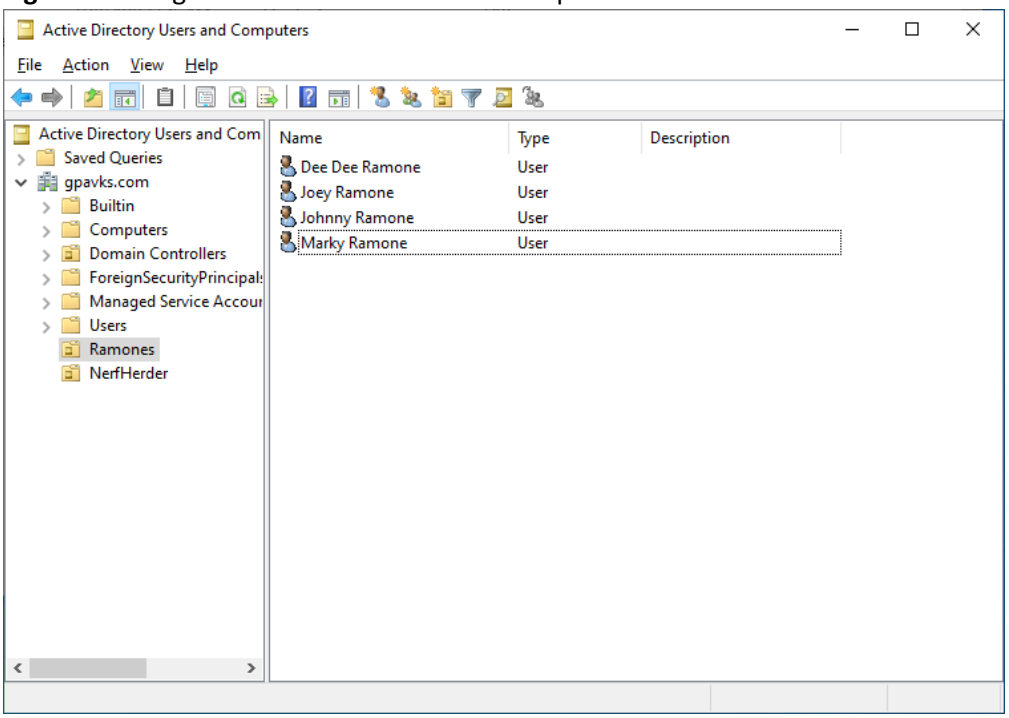
m. Using the **`Set-ADUser`** identifies the distinguished name of the AD object. There are generic parameters that are passed to the **`Set-ADUser`** cmdlet that can be used to modify the account. Below is a summary, for more information refer to the Microsoft PowerShell documentation.

- `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

Please Note: 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 in any way will be viewed as academic dishonesty, and you will fail the course.

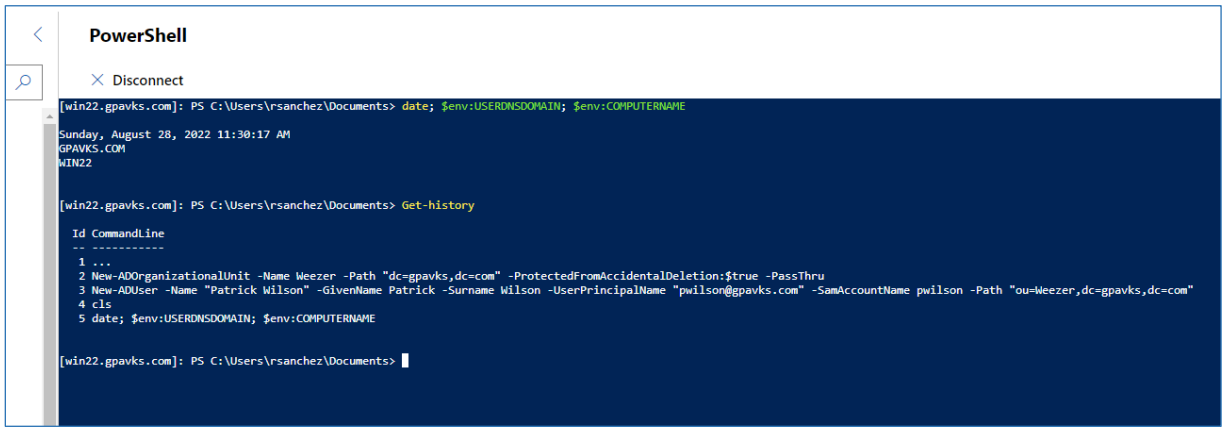
You must provide **TWO** screenshots of the information in the Active Directory Users and Computers. It must show the domain and the users created for **BOTH** Organizational Units, see Figure 71 for an example of one OU.

Figure 71 – 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 72). Use the **`date`**, **`$env:USERDNSDOMAIN`**, **`$env:COMPUTERNAME`**, and the **`Get-History`** cmdlets. You may split the screenshots if necessary.

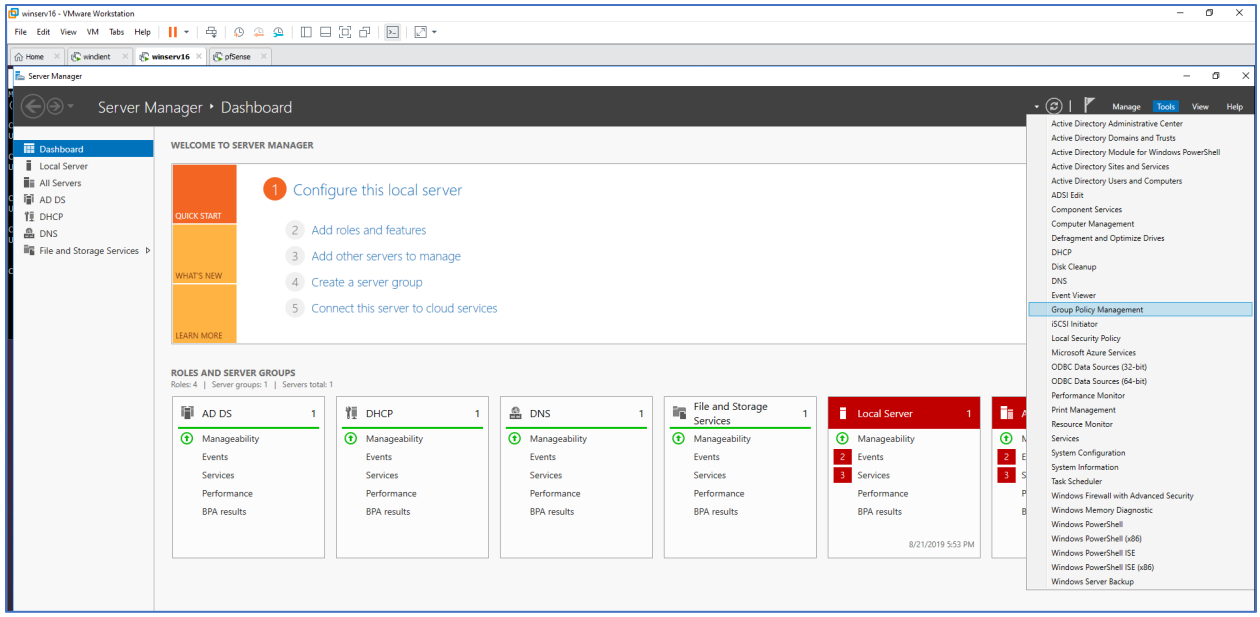
Figure 72 – Sample PowerShell History



Activity 6 – Creating and Linking a Group Policy Object

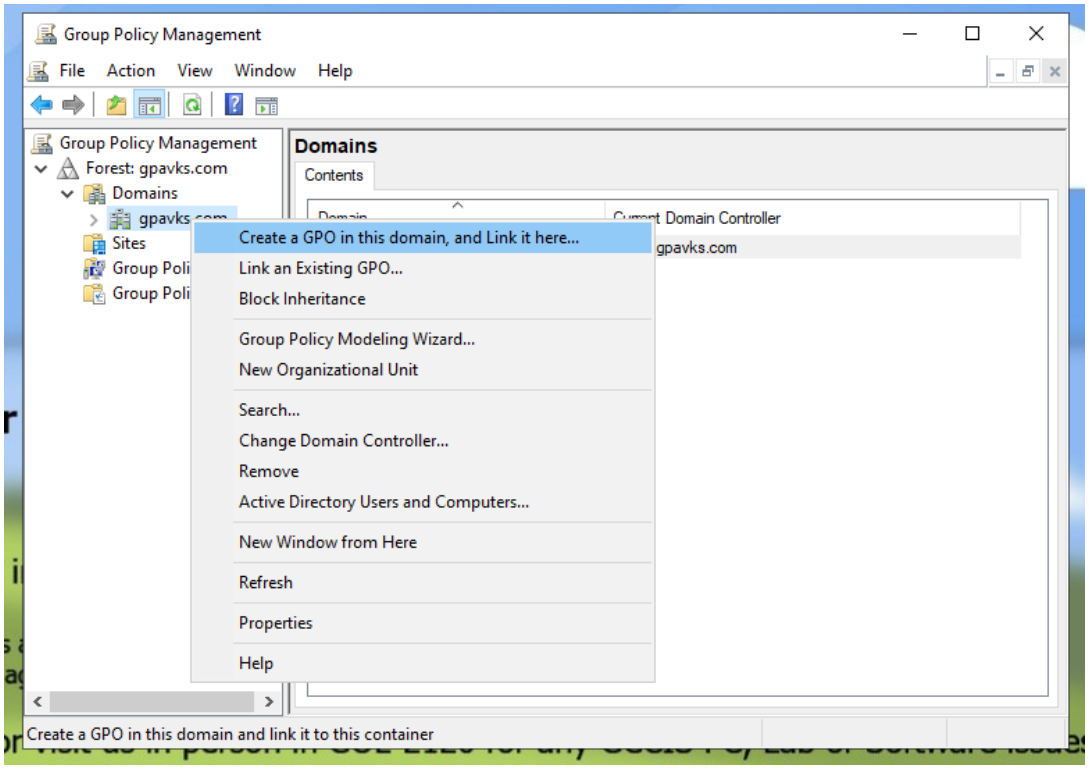
a. From the Server Manager Dashboard select *Tools* → *Group Policy Management* (Figure 73).

Figure 73 – Group Policy Manager



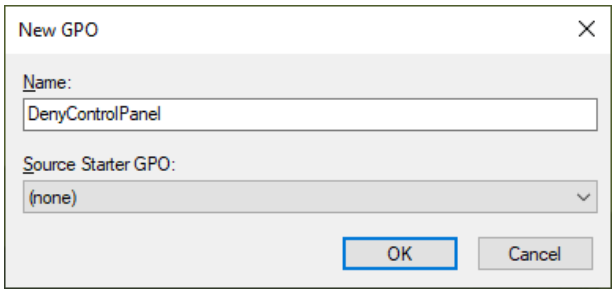
b. Expand the menu items to get to your domain. Right-click on the domain and select "*Create a GPO in this domain, and Link it here…*" (Figure 74).

Figure 74 – Creating a GPO



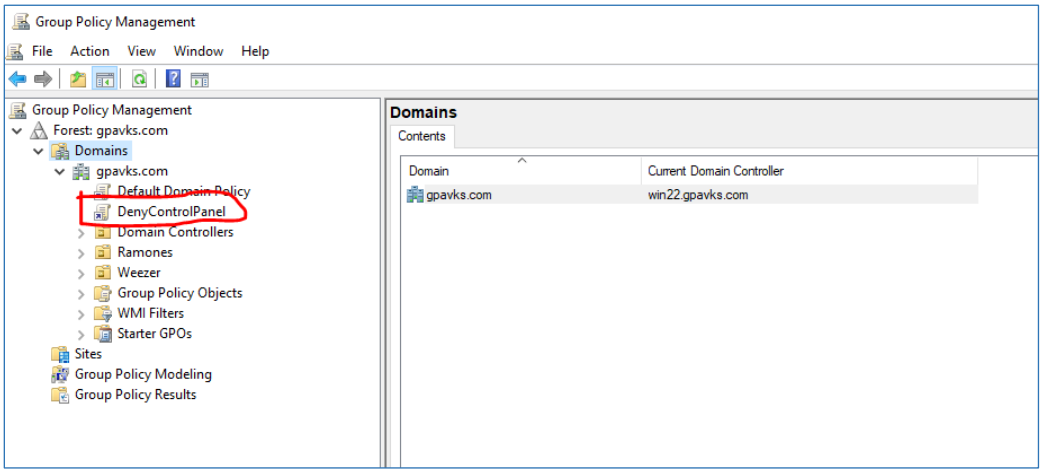
g. In the New GPO window, enter a name. In the example provided (Figure 75), I'm using "*DenyControlPanel*," to restrict user access to the Control Panel (Think "***Principal of Least Privilege***"). Name it whatever you like and click ***Ok***.

Figure 75– New GPO



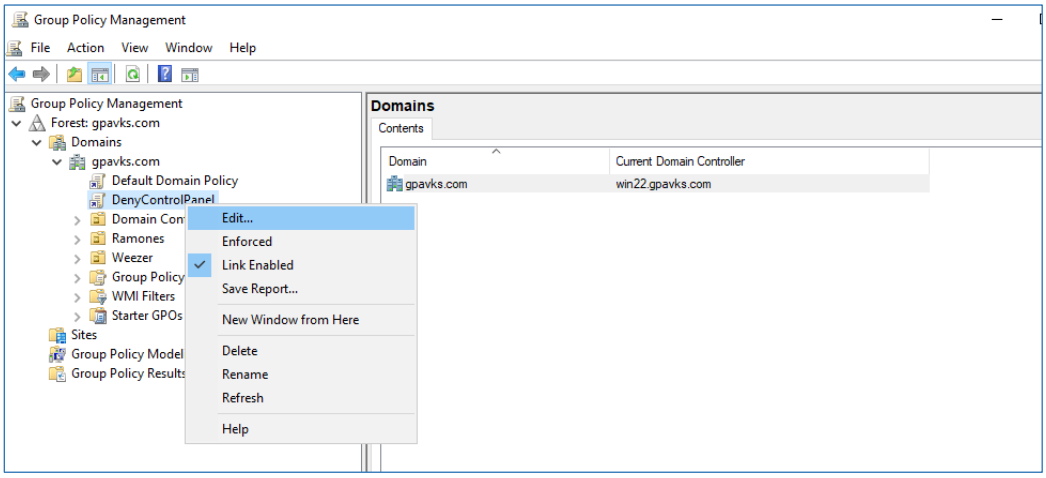
h. The Group Policy Object will be listed under the Domain (Figure 76).

Figure 76 – GPO



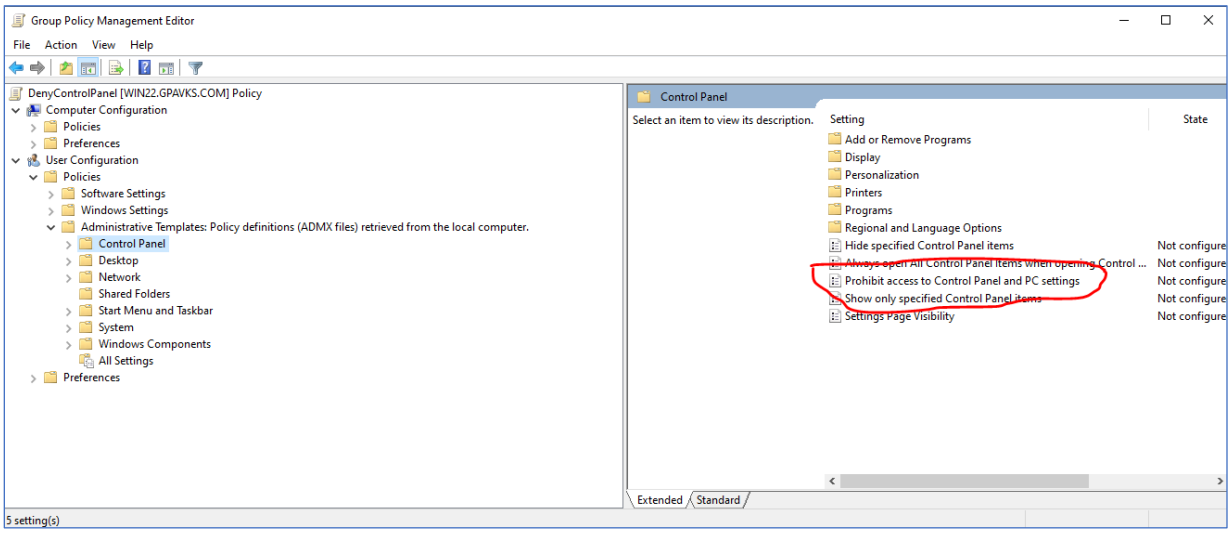
i. Right-click on the GPO and select ***"Edit"*** from the dropdown menu (Figure 77).

Figure 77 – Edit the GPO



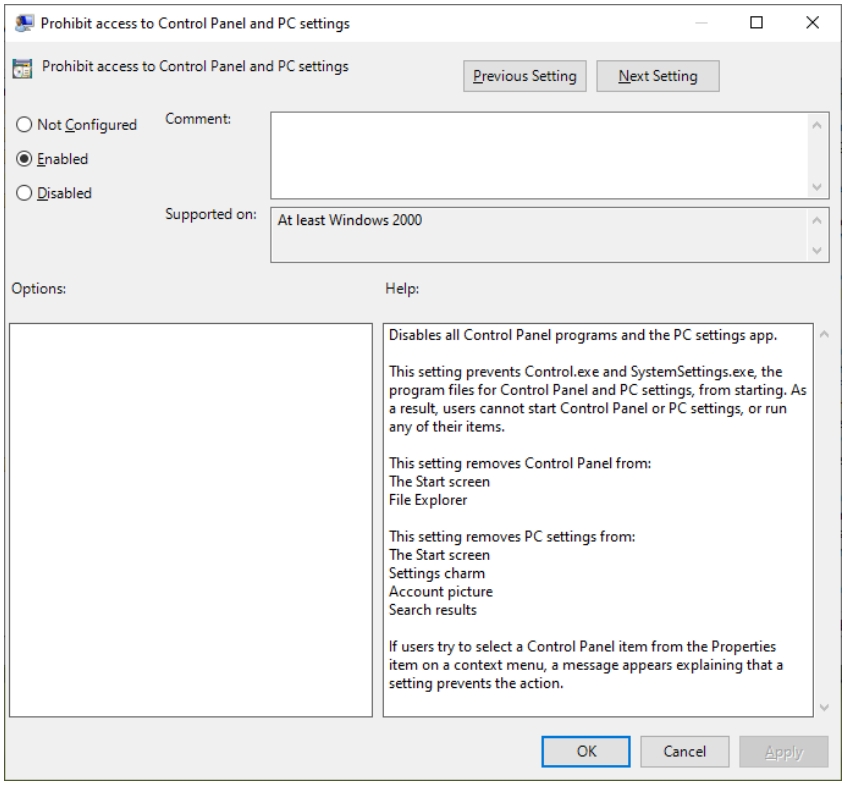
j. Next, navigate to *User Configuration → Policies → Administrative Templates, blah, blah, blah*, and the Control Panel folder. In the right pane, double-click "*Prohibit access to Control Panel and PC settings*" (Figure 78).

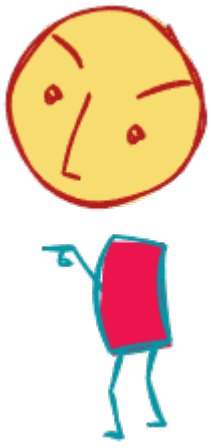
Figure 78 – Configuring GPO



k. The "Prohibit access to Control Panel and PC settings" window will appear. Select "*Enabled*", click ***Apply*** and then ***OK*** (Figure 79).

Figure 79 – Enable GPO



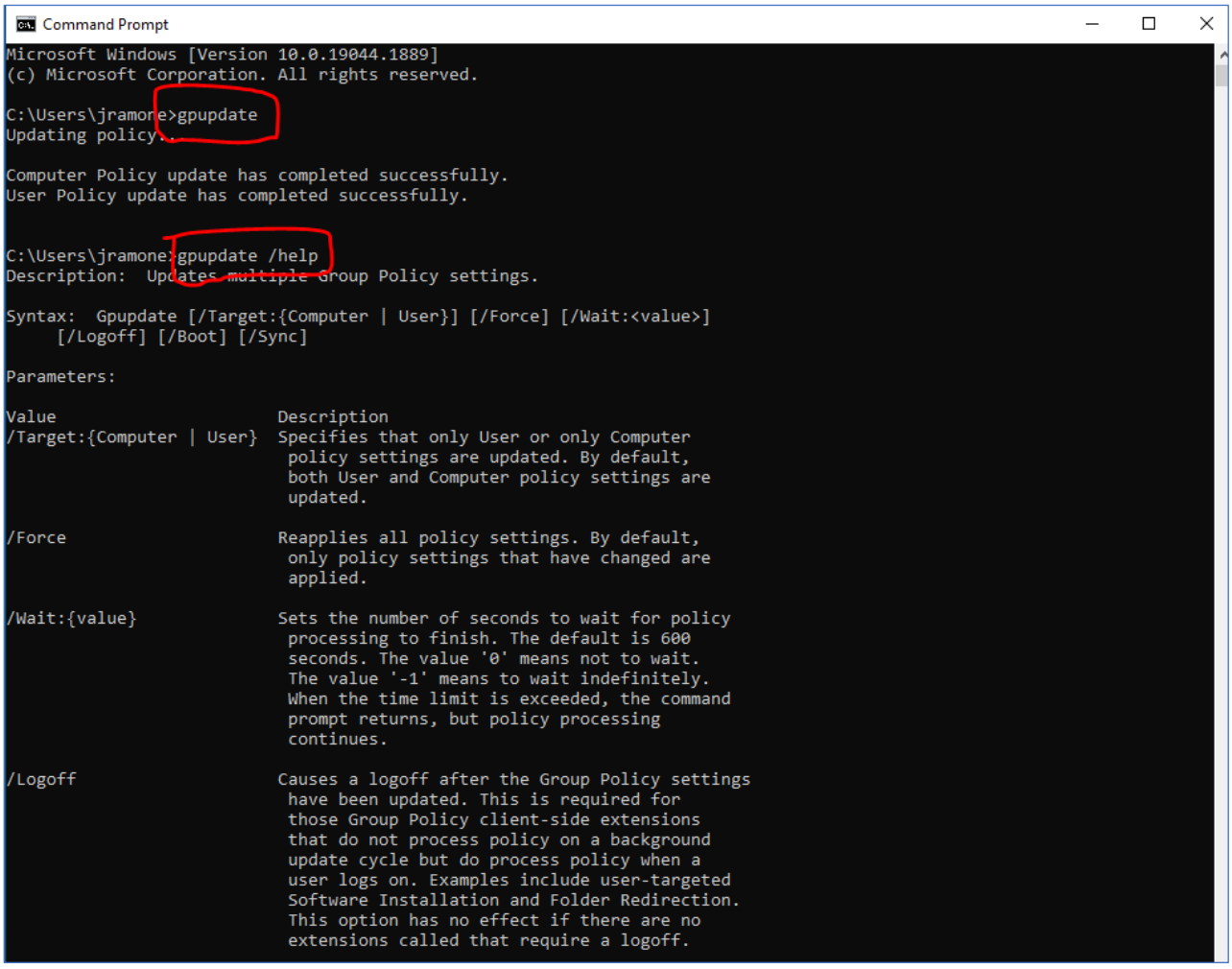


l. Return to the Windows 11 client and login in using a ***domain user*** account (Not a domain admin). Do not use and account if the user is a member of the domain admin group, remember the domain admin inherits the hosts local policies so the GPO you just created only applies to domain users.

m. Open the Command Prompt and type the command **`gpupdate`** to update the policy for that user (Figure 81). You shouldn't need to if you just logged in but knowing the gpupdate command is a god thing, when using Group Policy Objects. You might want to read the Windows documentation for it, or use help.

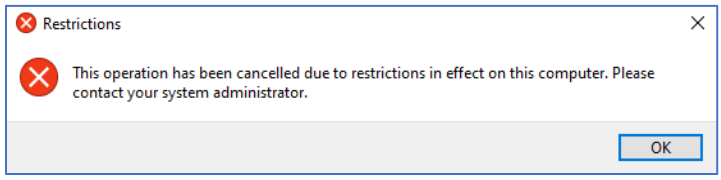
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate

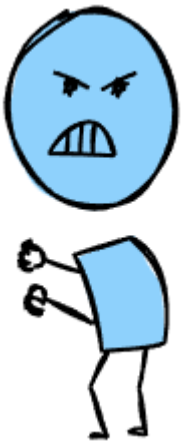
Figure 80 – Group Policy Update and Help



n. Try to access the control panel. You should receive the following message indicating that you are restricted from using it. (Figure 81).

Figure 81 – Restrictions





It's relatively common for companies to use a standard desktop wallpaper across all workstations in the organization. For this exercise, 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 can spare fifteen minutes, this YouTube video is helpful too.

https://www.youtube.com/watch?v=cWraXsgOJ7U

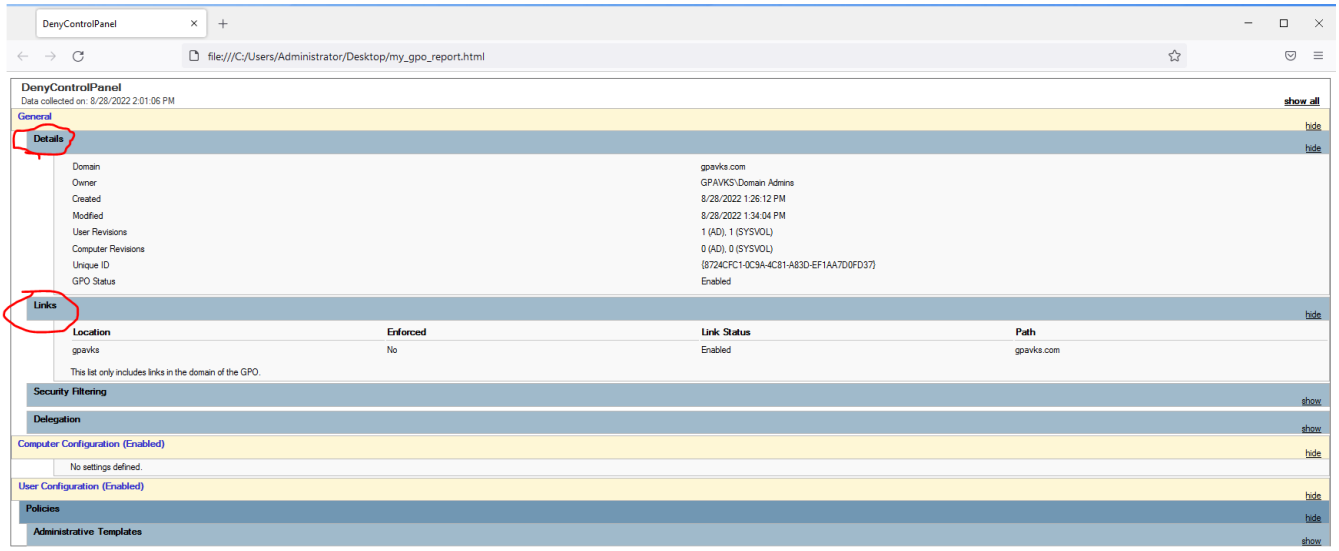
For the report include a screenshot showing the Group Policy Reports. Using Windows documentation and PowerShell create a report that shows the GPOs created in lab. Refer to Figure 82 for an example. Make sure to create reports for both GPOs, one for restricted access to the control panel and a second for the desktop. 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 and ***Links***.

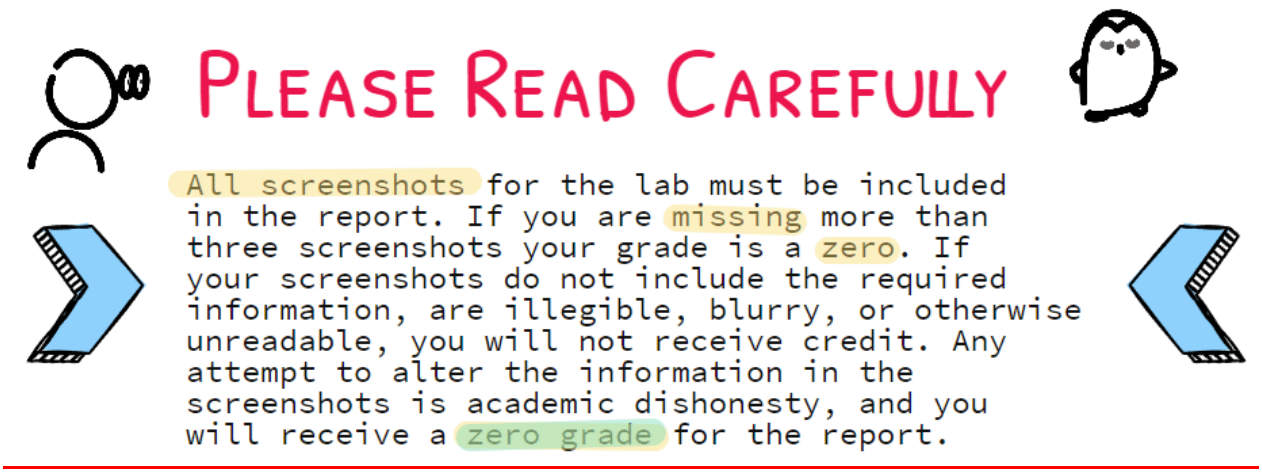
Windows PowerShell Documentation

https://docs.microsoft.com/en-us/powershell/module/grouppolicy/get-gporeport?view=windowsserver2025-ps&viewFallbackFrom=win11-ps

Please Note: The report is saved as an HTML document and will need to be viewed in a browser.

Figure 82 – GPO Report Example





Screenshot Summary

All screenshots must be labeled in the report using the following updated titles and descriptions:

1. **Figure 1 – Active Directory Validation**

   ☑ Output from PowerShell commands:
   date; Get-ADDomain
   Shows server validation and domain information.

2. **Figure 2 – Domain Controller and DHCP Scope Verification**

   ☑ Output from PowerShell commands:
   date; Get-DhcpServerInDC
   date; Get-Dhcpserverv4Scope
   Includes DHCP server details and scope information.

3. **Figure 3 – Windows 11 DHCP Validation**

   ☑ Screenshot of Windows 11 IP Configuration and Adapter Settings.
   Ensure visibility of:

   - Hostname
   - Primary DNS Suffix
   - DHCP lease information
   - DHCP server address
   - DNS server address

4. **Figure 4 – Windows 11 Domain Verification**

   ☑ Output from PowerShell commands:
   date; $env:COMPUTERNAME; (Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain
   Confirms Windows 11 client is a member of the domain.

5. **Figure 5 – Linux Domain Verification**

   ☑ Screenshot showing:

   - Current date
   - Logged-in user (whoami)
   - Hostname (hostname)
   - Domain membership using realm list --name-only

6. **Figure 6 – Active Directory Connection via Windows Admin Center**

   ☑ Screenshot showing successful connection to Active Directory through Windows Admin Center.
   Must display the FQDN of the server and the Active Directory Domain Service Preview.

7. **Figure 7 – PowerShell Session Output**

   ☑ Screenshot of remote PowerShell session using:
   date
   Get-ADDomain
   Verifies remote access and Active Directory information.

8. **Figure 8a – First Organizational Unit**

   ☑ Screenshot of the first Organizational Unit and users created using Windows Admin Center.

9. **Figure 8b – Second Organizational Unit**

   ☑ Screenshot of the second Organizational Unit and users created using PowerShell.

10. **Figure 9 – PowerShell History**

    ☑ Output of PowerShell history showing the creation of at least one user, including:

    - Commands used
    - $env:USERDNSDOMAIN
    - $env:COMPUTERNAME

11. **Figure 10a – GPO Report: Control Panel Restriction**

    ☑ HTML report screenshot showing the Group Policy Object restricting access to the Control Panel. Ensure inclusion of **Details** and **Links** sections.

12. **Figure 10b – GPO Report: Desktop Wallpaper**

    ☑ HTML report screenshot showing the Group Policy Object for setting the desktop wallpaper. Ensure inclusion of **Details** and **Links** sections.