European IT Certification Curriculum Self-Learning Preparatory Materials

EITC/IS/WSA

Windows Server Administration

This document constitutes European IT Certification curriculum self-learning preparatory material for the EITC/IS/WSA Windows Server Administration programme.

This self-learning preparatory material covers requirements of the corresponding EITC certification programme examination. It is intended to facilitate certification programme's participant learning and preparation towards the EITC/IS/WSA Windows Server Administration programme examination. The knowledge contained within the material is sufficient to pass the corresponding EITC certification examination in regard to relevant curriculum parts. The document specifies the knowledge and skills that participants of the EITC/IS/WSA Windows Server Administration certification programme should have in order to attain the corresponding EITC certificate.

Disclaimer

This document has been automatically generated and published based on the most recent updates of the EITC/IS/WSA Windows Server Administration certification programme curriculum as published on its relevant webpage, accessible at:

https://eitca.org/certification/eitc-is-wsa-windows-server-administration/

As such, despite every effort to make it complete and corresponding with the current EITC curriculum it may contain inaccuracies and incomplete sections, subject to ongoing updates and corrections directly on the EITC webpage. No warranty is given by EITCI as a publisher in regard to completeness of the information contained within the document and neither shall EITCI be responsible or liable for any errors, omissions, inaccuracies, losses or damages whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes in the document may be made by EITCI at its own discretion and at any time without notice, to maintain relevance of the self-learning material with the most current EITC curriculum. The self-learning preparatory material is provided by EITCI free of charge and does not constitute the paid certification service, the costs of which cover examination, certification and verification procedures, as well as related infrastructures.

TABLE OF CONTENTS

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: INTRODUCTION
TOPIC: GETTING STARTED

Welcome to this course on Windows Server Administration! In this course, you will gain practical experience in the IT field by performing tasks that IT professionals do every day.

The purpose of this course is to help you avoid the IT catch-22, where you struggle to find a job due to lack of practical experience, but are unable to gain experience without a job. This course will provide you with practical IT experience by guiding you through tasks that IT professionals perform daily. The best part is that you can do all of this from the comfort of your own home, using your own computer.

Windows Server is a fundamental component of most computer networks, and understanding its operating system is essential in the IT field. This course will not only teach you how to install Windows Server step-by-step through video lessons, but also guide you in setting up your own IT lab at home. By installing Windows Server on your own, you will gain firsthand experience and be able to explain the installation and configuration process to potential employers.

By the end of this course, you will have the practical experience necessary to confidently pursue a career in IT. So, let's not waste any more time. Click on the next lesson and let's get started!

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: VIRTUAL MACHINE FOR WINDOWS SERVER
TOPIC: DOWNLOADING AND INSTALLING VIRTUAL BOX

To download Windows Server 2016, follow the steps below:

1. Open your preferred web browser (e.g., Google Chrome).
2. Go to the website "tech net microsoft.com" and press enter.
3. Once the page loads, look for the "download" navigation button located at the top right, next to "home".
4. Click on the "downloads" link.
5. Under "TechNet downloads", you will find "Windows Server 2016" listed. Click on that link.
6. You will be redirected to the "Windows Server 2016 evaluation download" page.
7. If you do not have an account, you will be prompted to sign in or register. Create an account and sign in to continue.
8. Fill out the form with the required personal information. Note that this information will not be shown here for privacy reasons.
9. Click "continue" to proceed.
10. On the next screen, choose the file type you want to download. In this case, select "ISO" as it is the most commonly used in the IT field.
11. Click "continue".
12. Choose the language you prefer (e.g., English).
13. Click "download" to begin the download process.
14. Wait for the download to finish. The file will have a specific filename, so make sure to take note of it as it will be needed in future lessons.

Congratulations! You have successfully downloaded Windows Server 2016. We hope you found this lesson helpful, and we look forward to seeing you in the next one.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: VIRTUAL MACHINE FOR WINDOWS SERVER
TOPIC: DOWNLOADING WINDOWS SERVER

Virtualization is a key concept in the IT world that allows users to create a virtual computer within their existing computer system. This means that instead of erasing or splitting their hard drive to install a new operating system, users can create a virtual machine and launch it from their desktop. In this lesson, we will focus on downloading and installing VirtualBox, a software that enables virtualization.

To get started, open your web browser and go to virtualbox.org. Once the homepage loads, click on the Downloads link located on the left-hand side of the screen. Under the VirtualBox binaries, you will find different versions of VirtualBox depending on your operating system. If you are using Windows 7 or Windows 10, choose the Windows host version. If you are on a Mac, select OSX. For Linux users, there are specific options available as well. Note that the version number may vary, but this does not affect the functionality of the software.

After selecting the appropriate version, download the software. Once the download is complete, double-click on the executable file to start the installation process. Follow the installation prompts, clicking "Yes" and "Next" as needed. It is important to check the "Always trust software from Oracle Corporation" checkbox when prompted by the Windows security window. This step is crucial to avoid potential issues in the future.

Once the installation is complete, click "Finish" to finalize the process. Congratulations! You have successfully installed VirtualBox on your computer. In the next lesson, we will learn how to download the Windows Server 2016 operating system. Stay tuned for more information.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: VIRTUAL MACHINE FOR WINDOWS SERVER
TOPIC: WHAT IS A VIRTUAL MACHINE

A virtual machine (VM) is a software computer or a computer within a computer. It is essentially an entire computer that is stored on a physical hard drive. Similar to a physical server or machine, a VM can be powered on, an operating system can be installed, and various applications can be run on it. It can also be connected to internal networks.

The advantage of using a virtual machine instead of a physical server or machine is its portability. Since a VM is stored on the hard disk drive, it can be easily copied, duplicated, deleted, or moved at any time. This means that VMs can be transported across the internet without any time or cost constraints. For example, a virtual server can be easily transported from Washington DC to Hawaii.

Virtual machines are particularly useful in scenarios where multiple servers need to be created repeatedly. Instead of physically assembling a server and going through repetitive steps such as installing the operating system, updates, and software, a baseline virtual machine can be created. This baseline VM includes the operating system, updates, and necessary software. Whenever a new server needs to be deployed, the baseline VM can be cloned, tweaked as required, and deployed. This saves time and effort.

There are two important terms associated with virtual machines: hosts and guests. The host is the computer on which the virtual machine is installed, while the guest is the VM that runs on the host. A host can run multiple guest VMs, but a guest VM generally operates on a single host computer. It is important to note that a VM cannot have more resources (RAM, processing power, etc.) than its host computer. Therefore, the host computer needs to have sufficient physical resources to accommodate all the VMs.

In the example given, there is a single host computer running three guest VMs. The number of VMs that can be run on a host depends on the available physical resources. Typically, a VM will have a fraction of the total storage capacity and processing power of its host computer. To ensure optimal performance, it may be necessary to power off some VMs while others are turned on, especially when running VMs on personal computers with limited resources.

A virtual machine is a software computer that can be stored on a physical hard drive. It offers the advantage of portability and ease of deployment compared to physical servers. Hosts and guests are important terms associated with virtual machines, where hosts are the computers on which VMs are installed, and guests are the VMs that run on the hosts. Understanding these concepts is essential for successfully working with virtual machines.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: VIRTUAL MACHINE FOR WINDOWS SERVER
TOPIC: CREATING A VIRTUAL NETWORK WITH VIRTUAL BOX

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: VIRTUAL MACHINE FOR WINDOWS SERVER
TOPIC: CONFIGURING THE VIRTUAL MACHINE

In this lesson, we will learn how to connect a virtual machine to a virtual network and mount an ISO file in VirtualBox. Mounting an ISO file means virtually inserting a CD into a virtual computer.

To begin, open VirtualBox and select the virtual machine (VM) that you want to connect the ISO file to. Right-click on the VM and choose "Settings" or press Ctrl + S. In the Settings window, go to the "Storage" tab on the left-hand side.

Under the "Attributes" section, you will see an empty disk icon. Click on it and a drop-down menu will appear. From the drop-down menu, select "Virtual Optical Disk File". This will allow you to choose the ISO file that you downloaded earlier. Click "Open" to select the file.

Next, navigate to the "Network" tab by clicking on it on the left-hand side. Under "Adapter 1", you will see that the network adapter is already enabled and attached to a network. However, we need to change the network type to "Not Attached". To do this, click on the drop-down menu and select "Not Attached".

If you have previously created a NAT network, you will see it listed in the drop-down menu. Choose the appropriate network if you have multiple options. If you only have one network, it will be automatically selected. It is recommended to clean up any unnecessary networks for future use.

Once you have made these configurations, click "OK" to save the changes. The virtual machine is now configured to be connected to the NAT network and the Windows Server 2016 ISO file is mounted.

In the next lesson, we will learn how to install Windows Server on the virtual machine and proceed with its configuration.

Congratulations on completing this lesson! We look forward to seeing you in the next one.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH WINDOWS SERVER
TOPIC: INSTALLING WINDOWS SERVER

In this lesson, we will guide you through the process of installing Windows Server 2016. Before we begin, please ensure that you have completed all the necessary preparations for your virtual machine (VM), such as mounting the ISO file and attaching it to your network. Once you have done this, you can proceed with the installation process.

First, open VirtualBox by clicking on the VirtualBox icon in your taskbar. Select the VM you want to install Windows Server 2016 on, and click on the "Start" button. The VM will start up, and you can maximize the window for better visibility.

Next, you may notice that the VM does not have the VirtualBox Guest Additions tools installed. To scroll up and down within the VM, simply drag the bar on the side of the window.

Now, let's proceed with the installation. Under the "Language install" section, leave the settings as "English United States" and "US" for the keyboard method. It is important to choose the correct keyboard method to avoid any issues. The default settings are usually fine, so click on the "Next" button.

On the next screen, click on the "Install now" button to start the setup process. This may take a few moments, so please be patient.

Once the setup process begins, you will have the option to choose the version of Windows Server you want to install. Unlike Windows Server 2012, there is no longer an option for "Server with a GUI." Instead, it is now called "Desktop Experience." If you choose "Desktop Experience," you will install the full version of Windows Server with a graphical interface. If you choose not to install "Desktop Experience," you will install what is known as "Server Core," which requires the use of the command line for tasks and does not have a graphical interface. For this installation, we will choose "Datacenter Desktop Experience" since we are using a trial version.

After selecting the appropriate version, click on the "Next" button. On the next screen, you will need to accept the license terms by clicking on the "Next" button again.

The following screen will prompt you to choose the type of installation you want. If you already have Windows Server 2012 installed, you may choose the "Upgrade" option, which will preserve your files and settings. However, it is generally recommended to perform a fresh or custom installation whenever possible. In this case, since we do not have an operating system already installed on the VM, we will choose the "Custom: Install Windows only" option.

Now, you need to select the drive on which you want to install the operating system. If you have multiple drives or would like to create partitions, you can do so by clicking on the "New" button. For this installation, we will select "Drive 0" and click on the "Next" button.

At this point, the installation process will begin. It will prepare for the installation, complete the installation, and finalize some settings. This may take some time, so we recommend fast-forwarding the video or pausing it until the installation is complete.

Once the installation is finished, you will be prompted to set a password for the built-in administrator account. It is crucial that you remember this password, so please make sure to write it down or take note of it. Enter your desired password and press "Enter" on the keyboard.

The computer will then finish finalizing some settings, and you will be brought to the login screen. To log in with the administrator credentials you just created, press "Right Ctrl + Delete" on your keyboard. If you are using a Mac, press "Host + Delete." Enter the password you just set, and you will be logged in, bringing you to the desktop.

Congratulations! You have successfully installed Windows Server 2016. In the next lesson, we will cover the final steps of the installation process, including installing VirtualBox Guest Additions. Great job on completing this lesson, and we look forward to seeing you in the next one.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH WINDOWS SERVER
TOPIC: BASIC WINDOWS SERVER CONFIGURATION

To install the VirtualBox guest additions on a new server, as well as configure a static IP address and rename the server, follow these steps:

1. Open VirtualBox and select the VM that was created earlier.
2. Start the VM by clicking on the start button.
3. Enter the password that was created earlier and press Enter.
4. Wait for the desktop to load.
5. Install the VirtualBox guest additions CD image by going to Devices and selecting "Insert Guest Additions CD image".
6. Open the Windows Explorer and select the option to view files.
7. Double-click on the VirtualBox Windows Guest Edition application to start the installation.
8. Accept the default settings and click Next.
9. During the installation, there may be pop-ups asking to install certain drivers. Always select yes and make sure to check the box to trust Oracle software.
10. After the installation is complete, choose to manually reboot later and click Finish.
11. Configure a static IP address by selecting the local server and right-clicking on the Ethernet adapter. Click on Properties.
12. Uncheck IP version 6 and select IP version 4. Click on Properties.
13. Choose the option to use the following IP address.
14. Set the IP address to the same network as the NAT network, for example, 192.168.0.10.
15. Leave the subnet mask as default and set the default gateway to 192.168.0.1.
16. Set the preferred DNS server to either 127.0.0.1 or 8.8.8.8 (Google's DNS server).
17. Click OK and close the window.
18. Rename the computer by selecting the computer name under local server in Server Manager.
19. Click on Change and enter a new computer name, such as ITFDC01 (IT Flea Domain Controller 01).
20. Click OK and restart the computer.
21. Log back in once the computer has restarted.

In this lesson, we will cover the basic configuration of a Windows Server. To begin, let's focus on adjusting the resolution of the server. If the resolution is not fitting within the window, the server will automatically make the necessary adjustments. You can also enter full-screen mode by pressing right Ctrl + F. In full-screen mode, the file and VirtualBox options will be located at the bottom of the screen for easier access.

To ensure that our server is connected to the network, we will open the command prompt. To do this, click on the Start button and type "CMD" to open the command prompt program. It is recommended to right-click and pin it to the taskbar for easy access in the future.

Once the command prompt is open, we can test the network connection by pinging google.com. Simply type "ping google.com" and check if you receive a reply. If you do, it means that the virtual machine is connected to the internet and has a static IP address.

To verify the IP address of the virtual machine, you can type "ipconfig" in the command prompt. The IP address will be displayed, and in this case, it is set as 192.168.0.1, which is the IP address for the NAT network.

Congratulations on completing this lesson! You have successfully configured the basic settings of a Windows Server. We look forward to seeing you in the next lesson.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH WINDOWS SERVER
TOPIC: LAUNCHING WINDOWS SERVER

Windows Server 2016 is a powerful operating system commonly used by system administrators to manage servers. One of the primary tools for server management is Server Manager, which is included with all versions of Windows Server. To launch Server Manager, you can either wait for it to start automatically when the operating system starts, or you can click the Windows button and select Server Manager.

Server Manager allows you to manage your local server as well as other servers on your local network. It provides a wide range of management capabilities, including managing the computer name, IP address, firewall settings, Windows updates, events, services, and more. The left pane of Server Manager displays various sections, such as the dashboard, local server, all servers, and file and storage services.

The dashboard provides a quick overview of your server and allows you to configure it quickly. If there are any issues with the local server or remote servers, such as a service that failed to start, you will see them on this screen. To view errors with remote servers, you need to add them as remotely managed servers, and they will be shown under the all servers section.

The local server tab in Server Manager provides detailed information about the server you are currently logged on to. This tab allows you to change various settings, such as the computer name, domain membership, firewall, and network settings. It also displays events and services in more detail compared to the dashboard.

The all servers tab allows you to view the same events, services, and other information as the local server tab, but you cannot change the computer properties. The last tab, file and storage services, is a server role that includes technologies for setting up and managing file servers. These file servers provide central locations on your network where you can store and share files with other users.

In addition to understanding Server Manager, it is important to be familiar with two key terms: server roles and features. A server role is a set of software programs that allow a server to provide a specific service to its network. For example, adding a DHCP role to a server enables it to act as a DHCP server. On the other hand, features are individual software programs that can be installed independently or required by roles. You can add or remove roles and features by selecting the manage button in the top right-hand corner of the Server Manager window and choosing either add or remove roles and features.

When adding or removing roles and features, you will be presented with the before you begin tab, which provides informational content. After reading it, you can check the skip this page by default checkbox and proceed to the installation type tab. This tab offers two options: installing roles and features on a single server or installing roles on a virtual machine. For most scenarios, the first option is the most common and suitable choice.

The server roles tab allows you to select the roles you want to add to the server. If you only want to install features, you do not need to check any checkboxes in this tab. For the purpose of this lecture, we will install and uninstall roles and features to understand how it works. As an example, we will choose the fax server role, which requires additional features to be installed. Clicking the add features button and proceeding to the next step will allow you to install the required features.

The features tab in the add roles and features window is similar to the server roles tab. Here, you can select additional features to install if needed. Once you have made your selections, you can click Next to proceed with the installation process.

Server Manager is a powerful tool for managing Windows Server 2016. It allows you to manage local and remote servers, configure settings, view events and services, and more. Understanding server roles and features is essential for effectively working with Windows Server 2016, as they enable servers to provide specific services and offer additional software programs.

In order to work with Windows Server, it is important to understand how to launch and manage server roles and features using Server Manager. Server roles are sets of software programs that provide specific functionality to the server, while features are additional software components that can be installed to enhance the server's capabilities.

To begin, open Server Manager and navigate to the "Server Roles" tab. It is necessary to select at least one server role or feature to proceed. However, it is not mandatory to install any server roles. If no roles are selected, the installation process cannot proceed. It is worth noting that the required features for the selected server role are automatically checked for installation. Clicking "Next" will allow the installation process to continue.

The next screen will prompt you to select the server role you wish to install. When adding a new server role, informational tabs may be added to the wizard. Click "Next" through the prompts until you reach the "Server Role Services" tab. Here, you can check additional services if desired. For the purpose of this example, we will not include any optional role services. Click "Next" to proceed.

You will then be brought to the "Confirmation" tab. At this point, you have the option to check the "Restart the destination server" checkbox. It is generally recommended to check this checkbox. However, for the purpose of uninstalling the role immediately, it is left unchecked. Click "Install" to begin the installation process.

After clicking "Install," the results window will appear. It is important to note that you may close this wizard at any time, and the installation will still continue. To view the progress, click on the flag icon located at the top right-hand corner of Server Manager. Once the installation is complete, refresh Server Manager by either pressing F5 or clicking the refresh button next to the notifications button.

Upon refreshing, you will see a new notification stating that post-deployment configurations must be completed. Nearly every role installed will require some type of post-deployment configuration. However, since we are planning to uninstall this role, there is no need to complete this step.

To uninstall the newly installed role, click on "Manage" and select "Remove Server Roles and Features." Click "Next" through the prompts, choosing the same settings used during the installation process. When you reach the "Server Roles" tab, uncheck the "Fax Server" checkbox. A pop-up will appear, indicating that the features required by the server role can be removed. It is important to note that this list may not be exactly the same as the features required for installation. Click the "Remove Features" button and uncheck the "Print and Document Services" checkbox. Once again, you will be prompted to remove features that are required by the role. Click the "Remove Features" button.

Continue clicking "Next" until you reach the "Confirmation" window. This time, check the "Restart the destination server automatically if required" checkbox. When a warning message about the reboot appears, select "Yes." Click the "Remove" button and wait for the uninstallation process to finish. The server will then reboot.

Congratulations! You now understand how to use Server Manager to install and uninstall server roles and features in Windows Server 2016. This knowledge is essential for managing and configuring your server effectively.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH WINDOWS SERVER
TOPIC: ADDING THE ACTIVE DIRECTORY DOMAIN SERVICES ROLE IN WINDOWS SERVER

In this lecture, we will discuss how to create a domain controller by installing the Active Directory domain services (AD DS) role. Remember that any server running the AD DS role is considered a domain controller. We will add this role to our server and create a new domain called ITflea.com. However, you can use any name you prefer or use itecom2 if you want to keep things simple. It is important to note that creating a domain will not affect any external websites as there are no internet DNS servers pointing to the domain we are about to create.

To begin, you should already be familiar with how to install a server role on the server you are currently logged into. If not, don't worry, we will cover the steps again. Open Server Manager and select "Manage" followed by "Add Roles and Features". On the installation type screen, leave the default option "Role-based or feature-based" checked and click "Next".

In the server roles list, choose the "Active Directory Domain Services" role. A pop-up window will appear stating that you cannot install AD DS unless certain role services or features are also installed. Click the "Add Features" button and then click "Next" to proceed to the features screen. We do not need any additional features as all the required features have already been added. Click "Next" again.

You will now be brought to the AD DS screen, which informs us that we will also need to install the DNS role if it has not already been set up. Click "Next" and continue to the confirmation screen. Here, you can see the roles and features that will be installed. Click "Install" and wait for the installation to finish.

Once the installation is complete, there will be post-deployment configuration steps that need to be completed. Click the notification flag next to "Manage" and choose "Promote the server to a domain controller". The AD DS configuration wizard will appear, presenting us with three options.

The first option, "Add a domain controller to an existing domain", is used for adding additional domain controllers to a domain that has already been created. This option is not suitable for us since we have not yet created a domain.

The second option, "Add a domain to an existing forest", is used for adding a child or subdomain. In our case, we are creating a domain called ITflea.com. If this domain already existed, we could create a subdomain called "courses.ITflea.com". This would allow us to separate our students and teachers from our administrators and developers who reside in the domain ITflea.com. However, this option is not appropriate for us at the moment since the ITflea.com domain does not yet exist.

The third option is to "Add a new forest". This option allows us to create and specify a new domain. Choose this option and specify a root domain name. In our case, we will enter "ITflea.com" and click "Next".

After a moment, the domain controller options screen will appear. The first two options, "Forest functional level" and "Domain functional level", specify the operating system the domain controller will use. In this case, we are using Windows Server 2016. However, please note that there is a bug with the latest version of Windows Server 2016 where the screen may display "Windows Server Technical Preview" instead. If you see "Windows Server 2016", choose that option. Otherwise, choose "Windows Server Technical Preview".

Make sure that the "Domain Name System (DNS) server" checkbox is checked. This is necessary for the domain controller to function properly. The "Global Catalog" option ensures that the server will list all Active Directory objects. This is a requirement for the primary domain controller or when creating a new domain forest.

Do not check the "Read-only domain controller" option as it will prevent the domain controller from making changes to the domain. Type in a DSRM password and make sure to either write it down or memorize it. The DSRM password allows an administrator to take an instance of Active Directory offline for maintenance or troubleshooting purposes. While this is not commonly used, it is important to keep the password secure.

That concludes the process of adding the Active Directory domain services role in Windows Server. Remember to complete the post-deployment configuration steps after the installation is complete.

To add the Active Directory domain services role in Windows Server, follow these steps:

1. Open the Server Manager by clicking on the Start button and selecting "Server Manager".
2. In the Server Manager window, click on "Manage" in the top-right corner and select "Add Roles and Features".
3. The Add Roles and Features Wizard will open. Click "Next" on the Before You Begin screen.
4. Select "Role-based or feature-based installation" and click "Next".
5. Choose the appropriate server from the server pool and click "Next".
6. Scroll down and select "Active Directory Domain Services" from the list of roles. A pop-up window will appear, click "Add Features" to include the required features for Active Directory Domain Services.
7. Click "Next" on the Active Directory Domain Services screen.
8. Review the information on the Features screen and click "Next".
9. On the AD DS screen, read the information and click "Next".
10. Review the information on the DNS Options screen. Note that enabling DNS delegation will prevent external access to local DNS names, which is desired for security reasons. Click "Next" to proceed.
11. On the Additional Options screen, the NetBIOS name will be automatically populated. This is an abbreviated version of the fully qualified domain name (FQDN). Leave it at the default setting and click "Next".
12. On the Paths screen, the default path for the required folders will be shown. If desired, an alternative path can be chosen by clicking the "..." button. It is recommended to leave the settings at the default and click "Next".
13. The Review Options screen will show all the chosen options. If desired, the PowerShell script can be viewed by clicking the "View script" button. This script can be saved and used to quickly complete the wizard with the same settings. Close the PowerShell script and click "Next".
14. The Prerequisite Check window will verify if the server is ready to be promoted as a domain controller. This process may take a few minutes. Once the checks are complete, all prerequisite checks should pass. If any errors occur, they can be resolved by searching for the specific error online and following the instructions to fix it. Once the errors are fixed, click the "Rerun prerequisites check" link and wait for the checks to finish again.
15. Under the View Results window, various warnings may be displayed. These warnings are not critical, but it is recommended to read through them. Some warnings may include security settings related to old technology or networking adapter configurations. These warnings can be ignored for this setup.
16. Click the "Install" button and wait for the installation to complete. The server will then reboot, which may take some time depending on the server's speed.
17. Once the installation is complete and the server reboots, press Ctrl+Alt+Delete to log in.
18. Log in using the NetBIOS name of the domain followed by the administrator account. For example, if the NetBIOS name is "ITFLEA" and the administrator account is "administrator", enter "ITFLEA\administrator" as the username.
19. Enter the password used to create the administrator account during the initial server installation and click "OK".
20. Once the desktop loads and Server Manager opens, you will notice the new roles "AD DS" and "DNS". This indicates that the domain controller has been successfully built.

Congratulations on completing the process of adding the Active Directory domain services role in Windows Server!

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH WINDOWS SERVER
TOPIC: JOINING OUR WORKSTATION TO OUR DOMAIN IN WINDOWS SERVER

To join a Windows 10 workstation to a domain in Windows Server, follow these steps:

1. Open VirtualBox and ensure that both the domain controller and the Windows 10 VM are powered on and connected to the same network.
2. Verify that the network settings for both the domain controller and the Windows 10 VM are set to NAT Network.
3. Restart the Windows 10 VM to apply any hardware or settings changes made in VirtualBox.
4. After the VM has booted up, press Ctrl+Alt+Delete to access the login screen, enter your password, and log in.
5. If the resolution is not automatically adjusted, minimize the VM window and resize it to allow for dynamic resolution.
6. Enter full-screen mode by pressing Ctrl+F and click on the Start button in the bottom left corner.
7. Type "CMD" to open the command prompt.
8. Check the IP configuration using the "ipconfig" command. If the IP address starts with 169, it means that the VM is not reaching the DHCP server.
9. Run the "ipconfig" command again. This time, the IP address should start with 10.0.2.7, which is not on the same network as the domain controller.
10. VirtualBox's DHCP server only assigns IP addresses in the 10 subnet, regardless of the actual network. To resolve this issue, we need to manually change the IP version 4 settings.
11. Click on the Start button, go to Settings, and select Network & Internet.
12. Click on "Change adapter options" at the bottom, right-click on Ethernet, and choose Properties.
13. Uncheck IP version 6 and select Internet Protocol version 4. Click on Properties.
14. Choose the option to use the following IP address and enter 192.168.0.100 as the IP address.
15. Press Tab to automatically fill in the subnet mask.
16. Set the default gateway to 192.168.0.1, which is usually the router's IP address.
17. Close all windows and go back to the command prompt.
18. Verify that the default gateway assigned by DHCP is the same as the one entered in the IP settings.
19. At this point, the Windows 10 workstation is ready to be joined to the domain. Follow the appropriate steps to join the domain.

By following these steps, you can successfully join a Windows 10 workstation to a domain in Windows Server.

To join a workstation to a Windows domain, there are several steps that need to be followed. First, we need to configure the IP address and DNS server settings correctly. The IP address should be the one assigned to the networking switch that the workstation is connected to. The preferred DNS server should be the IP address of the DNS server on the network, which in our case is the IP address of the domain controller (192.168.0.1).

Once the IP address and DNS server settings are configured, we need to ensure that we are on the same network as the domain controller. This can be verified by running the "ipconfig" command and checking if we have an IP version 4 address in the same network range (192.168.0.0).

However, it is important to note that by default, the Windows Firewall on the domain controller will block ping requests. So, if we try to ping the IP address of the domain controller (192.168.0.1), we may receive a "destination host unreachable" or a timeout message. This is normal behavior, and it does not mean that the connection is not established.

Next, we need to rename the computer to a desired name. This can be done by going to the "Settings" menu, selecting "System," and then choosing "Rename this PC." In the "Rename this PC" window, we can enter the desired name for the workstation, such as "ITF-WS01" for an IT fleet workstation. After entering the name, we can proceed to the next step.

To join the workstation to the domain, we need to go to the "Connect to work or school" section in the "Settings" menu. Under the "Connect" option, we should select "Join this device to a local Active Directory domain." In the domain field, we need to enter the name of the domain, which in our case is "ite.com." After clicking "Next," we may be prompted to enter an account with administrative permissions to connect to the domain. In this case, we should enter the administrator account and password that was created during the installation of Windows Server 2016.

Once the account is verified, the computer will restart. After the restart, the workstation will be joined to the domain. To confirm this, we can switch to the domain controller and log in using the domain administrator account. From the "Active Directory Users and Computers" tool, we can navigate to the "Computers" container under the "ITFlea.com" domain and verify that the workstation (ITF-WS01) is listed.

At this point, the workstation is successfully joined to the Windows domain, and further configuration and management can be done, such as assigning Group Policy Objects (GPOs) to the workstation.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: DEPLOYING WINDOWS
TOPIC: DOWNLOADING WINDOWS 10

In this lecture, we will discuss the process of downloading a Windows 10 ISO installation file from Microsoft. An ISO file is a disk image that can emulate a CD or DVD. Although this file cannot be natively opened on Windows, we can use VirtualBox to read the ISO and extract the Windows installation files from it.

To begin, open your preferred web browser on your host computer and navigate to google.com. In the search bar, type "Windows 10 download tool" and press Enter. This will direct you to the Microsoft software downloads page, where you can find the Windows 10 media creation tool. Open this page and wait for it to load.

Once the page has loaded, click on the "Download now" button to initiate the download process. Allow the download to complete, and then launch the installer file. Follow the prompts and accept the license terms to proceed.

On the following screen, select the option to "Create installation media for another PC" and click "Next". You can choose to leave the default settings or customize them by unchecking the "Use the recommended options for this PC" checkbox. For this tutorial, we will stick with the default settings and click "Next".

On the next screen, check the "ISO file" checkbox. This option allows us to download an ISO file that we can later mount to a virtual machine (VM) and use to install Windows 10. Click "Next" to continue.

Choose a location where you want to save the new ISO file. It is recommended to change the name from "Windows.iso" to something like "Windows 10.iso" to avoid confusion with other ISO files in the future. Once you have selected the location and renamed the file, click "Save".

Now, all you need to do is wait for the download to finish. Once it is complete, you will have successfully downloaded the Windows 10 ISO installation file from Microsoft.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: DEPLOYING WINDOWS
TOPIC: INSTALLING WINDOWS 10

In this lesson, we will learn how to create a Windows 10 virtual machine (VM) and install Windows 10 using VirtualBox.

To begin, open VirtualBox and click on the "New" button in the top left corner of the screen. If you see the guided mode, click on the "Expert Mode" button at the bottom.

Next, enter a name for the VM (e.g., Windows 10 VM) and select Windows 10 as the version. The minimum recommended RAM size will be automatically calculated as 2 gigabytes. Leave the option to create a virtual hard disk and select "Create." Change the disk size to 80 gigabytes and choose the VDI format. Make sure to select "Dynamically allocated" for the disk storage. Click on "Create" to create the VM.

Now, we need to configure the network settings for the VM to be on the same network as the domain controller and mount the Windows 10 ISO file. Right-click on the VM, choose "Settings," and go to the "Network" section. Change the network attachment to "NAT Network" if your domain controller is using a NAT network. If you are using a host-only or internal network, select the corresponding option. Make sure to select the correct NAT network under the name.

Next, go to the "Storage" section and click on the empty disk icon on the left. On the right side, click on the disk icon and choose "Choose Virtual Optical Disk File." Select the Windows 10 ISO file and click "Open." Click "OK" to save the settings.

Now, we are ready to power on the VM and start the installation. Click on the "Start" button, and the VM will begin to power on. Since the VirtualBox guest additions are not installed yet, use the scroll wheel on the right side to scroll up and down.

First, ensure that the language, time, currency, and keyboard input method settings are correct. This is crucial to avoid input issues. Click "Next" to continue.

Choose "Install Now" to begin the setup. Select "I do not have a product key" and choose "Windows 10 Pro" (other editions may not be able to join a Windows 10 domain). Click "Next" and accept the license terms.

Select the "Custom" option as we are not upgrading an existing installation. Choose the default partition (Drive 0) and click "Next" to start the installation.

During the installation, there will be some waiting time. You can speed up the video or pause it until the installation is complete.

After the installation, you will need to configure some settings. Click "Yes" for the United States region and confirm the correct keyboard layout. Skip adding a second keyboard layout.

Choose "Skip" for now regarding the network settings. Enter your name and password for the VM. Create a password hint if needed.

Finally, decide whether to enable Cortana as your personal assistant. It is recommended to disable it for better performance in a test lab environment.

And that's it! You have successfully created a Windows 10 VM and installed Windows 10 using VirtualBox.

To install Windows 10 on a virtual machine, follow these steps:

1. After starting the virtual machine, select "No" when asked about using the VM for anything other than tests and lab purposes. This will disable speech recognition, tailored experiences, location diagnostics, and relevant ads, reducing resource usage and improving performance.

2. Once on the desktop, go to the "Devices" menu and select "Insert Guest Additions CD image". A pop-up will appear asking what happens with the disk. Click on it and choose "Run VBox Windows Edition CXC" from the top.

3. Proceed with the installation by clicking "Yes" and then "Next" through the prompts. The default options should work fine. Make sure to check the box that says "Always trust software from Oracle Corporation" and select "Install".

4. After the installation completes, click "Finish". The virtual machine will restart, and features like dynamic resolutions and copying and pasting between the VM and the host will now work properly.

That's it! You have successfully installed Windows 10 on your virtual machine. Enjoy exploring and experimenting with the operating system.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: DEPLOYING WINDOWS
TOPIC: INTRODUCTION TO WINDOWS DOMAIN AND DOMAIN CONTROLLER

A Windows domain is a system that allows system administrators to efficiently manage small or large computer networks. It has been around since 1993 with the release of Windows NT. To build a Windows domain, you only need one domain controller (DC). However, most domains contain several servers and computers.

A domain controller is any server that has the Active Directory Domain Services (AD DS) role installed. Its main job is to handle authentication requests across the domain. Domain controllers hold important tools such as Active Directory and Group Policy. These tools are used to create new user accounts, change domain policies, and manage various aspects of the network.

Within a domain, you can have multiple domain controllers. However, there is only one primary or main domain controller. The primary reason for having multiple domain controllers is fault tolerance. Critical information, such as user and account information, is replicated between the domain controllers. If one domain controller goes down, the client computers will switch to another functioning domain controller.

Active Directory Users and Computers (ADUC) is a tool commonly referred to as AD. It is used to manage user and computer accounts and also acts as a directory service for network resources like printers and file shares. When a domain user searches for a new printer to install, they will find all the printers that have been added to the domain controller with Active Directory.

AD allows management of various objects, including domain users, computers, printers, file shares, and groups. Groups contain members, which can be any valid AD object, such as a user or a computer. AD objects are stored within folders called Organizational Units (OUs).

Group Policy Management (GPM) is another important tool located on a domain controller. It allows administrators to manage all domain users or domain computers remotely. GPM uses Group Policy Objects (GPOs) to manage the settings of valid AD objects. With GPM, you can target specific AD objects, specific OUs, or the entire domain to create custom settings. It enables you to configure desktop backgrounds, manage website access in Internet Explorer, and control security settings, among countless other options.

To recap, a Windows domain is a way to manage computer networks efficiently. It utilizes a Windows server called a domain controller (DC), which responds to authentication requests across the domain. DCs have tools such as Active Directory and Group Policy. Active Directory contains objects and OUs, while Group Policy contains GPOs that manage settings for AD objects.

Great job on completing this lecture! There was a lot of information covered, so you may want to review it again. There will be a quiz on this topic later in this section. Keep up the good work, and I'll see you in the next lecture.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: CONFIGURING DHCP AND DNS ZONES IN WINDOWS SERVER
TOPIC: ADDING THE DHCP SERVER ROLE IN WINDOWS SERVER

In this lecture, we will learn how to create a DHCP server by installing the DHCP server role on our ITF DC 0 1 server. To begin, make sure you are logged into the domain controller. Open Server Manager and select "Manage" > "Add Roles and Features." Continue through the prompts until you reach the "Server Roles" tab. Check the DHCP server checkbox and click "Add Features" when prompted to add the required features for the DHCP server role. Click "Next" until you reach the confirmation window, then click "Install" to begin the installation process. Wait for the installation to complete.

Once the installation is finished, click the "Complete DHCP Configuration" text. If you have already closed the installation window, click the "Notifications" button at the top of the screen and select the DHCP notification. The DHCP post-install configuration wizard will appear. In the first window, you will be informed that you need to create the DHCP administrators and DHCP user security groups, as well as authorize the DHCP server.

On the authorization screen, specify a domain user account with domain administrative permissions. By default, the account "Administrator" is specified, which is a domain account indicated by the domain NetBIOS name "ITFLEE\" prefix. This account is suitable for the required tasks, so click "Commit" to continue.

Next, you will be brought to the summary page, where you can see the two tasks that have been completed. Close out of the DHCP windows. On the left side of the screen, you will notice a DHCP tab. Click on this tab to view information related to DHCP, such as events and services.

To open the DHCP management console, click on "Tools" > "DHCP" within Server Manager. The DHCP management console will appear, listing our server along with its IPv4 and IPv6 settings. In this course, we will focus on IPv4, as it is the most commonly used protocol. Please note that our DHCP server is not fully functioning yet, as we need to define a scope for it to use. We will cover this in the following lectures.

Congratulations on successfully installing the DHCP server! See you in the next lecture.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: CONFIGURING DHCP AND DNS ZONES IN WINDOWS SERVER
TOPIC: DHCP SCOPES AND EXCLUSIONS

A DHCP scope is a pool of IP addresses on a specific subnet that can be leased by the DHCP server. Each subnet can only contain one scope with a continuous range of IP addresses. This means that you cannot create multiple scopes with overlapping IP ranges. Instead, you need to create a single scope with a range that includes all the desired IP addresses and then create exclusions for any addresses that should not be leased.

To create a DHCP scope in Windows Server, open the DHCP management console by opening Server Manager and selecting Tools > DHCP. Right-click on the DHCP server you want to configure and select New Scope.

In the New Scope wizard, specify a scope name and description. The scope name and description are only for administrative purposes and are not visible to clients. Next, specify the start and ending IP addresses for the scope. It is important to ensure that the start and ending IP addresses fall within the same subnet and do not overlap with any existing scopes.

The length and subnet mask for the scope are automatically calculated based on the IP range specified. These settings can be left at their default values unless you have specific requirements.

Next, you have the option to specify any exclusions for the scope. Exclusions are IP addresses that should not be leased by the DHCP server. Excluded IP addresses must fall within the scope that was created. Enter the start and ending IP addresses for the exclusion range and click the Add button to add it to the list.

After specifying exclusions, you can configure the lease duration for the DHCP clients. The lease duration determines how long a client can keep the assigned IP address before it needs to renew the lease. The default lease duration is 8 days, but you can adjust this if needed.

You can also configure the default gateway, DNS server, and WINS server for the scope. The default gateway is the IP address of the router that provides access to other networks. The DNS server is responsible for resolving domain names to IP addresses. The WINS server is an outdated feature and is not commonly used anymore.

Finally, you have the option to activate the scope immediately or do it later. Activating the scope makes it available for lease to DHCP clients. Once the scope is activated, you can view and manage the address pool, address leases, reservations, scope options, and policies associated with the scope.

The address pool lists all the available IP addresses in the scope, including any exclusions. The address leases screen shows the client computers that have received a TCP/IP configuration from DHCP. Reservations list the computers that have a DHCP reservation, which is a specific IP address assigned to a particular client. Scope options allow you to configure additional network settings such as the default gateway and DNS servers. DHCP policies allow you to assign specific IP address ranges to certain devices based on criteria such as device type.

That concludes this lecture on creating a DHCP scope in Windows Server. You have learned how to configure the scope, specify exclusions, set the lease duration, and configure additional network settings. Great job!

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: CONFIGURING DHCP AND DNS ZONES IN WINDOWS SERVER
TOPIC: HOW DHCP WORKS IN WINDOWS SERVER

Dynamic Host Configuration Protocol (DHCP) is a networking protocol that automates the assignment of TCP/IP configurations to client computers on a network. By installing the DHCP server role on a Windows server, administrators can configure the IP address, subnet mask, DNS server address, and gateway of client computers automatically.

Before DHCP was implemented, system administrators had to manually configure the TCP/IP settings on each computer, which was time-consuming and prone to errors. DHCP eliminates these issues by assigning configurations to client computers for a lease period. Once the lease expires, the client computer must either renew its existing lease or obtain a new configuration and lease from the DHCP server.

To understand how DHCP works, let's consider an analogy with a hotel. When a person, let's call him Johnny, arrives at a hotel, he asks the desk clerk for a room. The clerk checks the registry to see which rooms are available. Some rooms may be excluded from DHCP, meaning they cannot be assigned to clients. This could be due to maintenance or other reasons.

The clerk also finds that certain rooms have been reserved for other guests. These rooms are not currently occupied, but they cannot be assigned to Johnny. Similarly, DHCP reservations reserve specific IP addresses for certain devices or computers. These addresses are not in use, but they are reserved for other clients.

The clerk then identifies rooms that are currently occupied and cannot be assigned to Johnny. In DHCP, computers can take available IP addresses as they become available.

Finally, the clerk finds a room, room 202, that is available for one week. This duration represents the DHCP lease, which specifies how long a client computer can keep an assigned IP address. The clerk assigns room 202 to Johnny, updates the registry to reflect the assignment, and ensures that no other client will receive the same room.

At the end of the week, if Johnny wants to stay in the hotel, he must request another week from the clerk. Similarly, when a client computer's DHCP lease expires, it contacts the DHCP server to either extend its lease with the same IP address or obtain a new IP address and lease. This process ensures efficient IP address management within the network.

Administrators can configure the range or scope of IP addresses to be supplied by DHCP and exclude specific IP addresses from assignment. This allows for better control and management of IP address allocation.

DHCP is a networking protocol that automates the assignment of TCP/IP configurations to client computers. By installing the DHCP server role on a Windows server, administrators can configure the IP address, subnet mask, DNS server address, and gateway of client computers automatically. DHCP leases IP addresses for a specified period, and clients must renew their leases or obtain new configurations when the lease expires.

DHCP (Dynamic Host Configuration Protocol) is a network protocol used in Windows Server to automatically assign IP addresses and other TCP/IP settings to client computers. This eliminates the need for manual configuration and makes it easier to connect new devices to a network.

In DHCP, the server is responsible for assigning IP addresses to client computers. This is different from manually configuring the IP address on the client computer itself. If a computer is unable to find a DHCP server on the network, it assigns itself a private IP address starting with 169.254.

Let's take a look at how DHCP works. In this example, we have two computers connected to a switch. The Windows workstation is not plugged into the switch yet, so it has assigned itself a private IP address. When we plug the network cable into the switch, the client computer starts broadcasting a DHCP discovery request to the entire network. It hopes to reach a DHCP server.

The DHCP server listens for this request and responds with a DHCP offer. The offer includes all the TCP/IP settings, such as the IP address, subnet mask, DNS server, and gateway. Once the client receives the offer, it sends back a DHCP request to the server, indicating that it wants to keep the offered settings. The server acknowledges the request with an acknowledgement message.

Now, let's recap the process. We can remember it with the acronym DORA: Discover, Offer, Request, and Acknowledgement. The client sends a DHCP Discover message, and the server responds with a DHCP Offer. The client then requests the offered settings, and the server acknowledges the request.

Static IP addresses are still relevant for certain devices, such as servers and printers. This is because one of the settings that DHCP can automatically configure is the DNS server. If the DNS server's IP address changes frequently, it would be cumbersome to update the DHCP settings every time. Assigning a static IP address to the DNS server ensures that it never changes.

Similarly, printers and scanners are often assigned static IP addresses so that users can consistently print to them without needing to re-enter the IP address. DHCP reservations can also be used to assign specific IP addresses to devices based on their MAC addresses. However, it's important to note that if the DHCP server crashes, a client computer with a DHCP reservation will lose its configured IP address when the lease expires.

DHCP is a network protocol used to automatically assign IP addresses and other TCP/IP settings to client computers. It simplifies the process of connecting new devices to a network. While DHCP is typically used for workstations, servers and printers often use static IP addresses to ensure consistent connectivity. DHCP reservations can be used to assign specific IP addresses to devices based on their MAC addresses.

DHCP (Dynamic Host Configuration Protocol) is a crucial component in Windows Server administration for managing IP addresses. In the event of a DHCP server crash, computers that rely on DHCP will remain connected until their TCP/IP lease expires. If a computer is configured to use DHCP but fails to find a DHCP server, it will assign itself a private IP address starting with 169.254.xx.xx.

Understanding the role of DHCP in Windows Server is essential for maintaining network connectivity and ensuring smooth operations. By automatically assigning IP addresses, DHCP simplifies network administration and eliminates the need for manual configuration on individual computers.

To summarize, DHCP plays a vital role in Windows Server administration by dynamically assigning IP addresses to devices on a network. It ensures that computers remain connected even in the event of a DHCP server crash and allows for efficient network management.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: CONFIGURING DHCP AND DNS ZONES IN WINDOWS SERVER
TOPIC: DHCP RESERVATIONS IN WINDOWS SERVER

In this lecture, we will learn how to create a DHCP reservation for a Windows 10 workstation with the IP address of 192.168.0.1. To create the reservation, we need to have our domain controller and Windows 10 VMs powered on.

The first step is to grab the MAC address from our Windows 10 workstation. We can do this by opening the command prompt on the Windows 10 VM. To open the command prompt, click the Windows button and search for CMD. Select the command prompt from the list.

In the command prompt, type the command "getmac" to grab the MAC address of our VM. Note that there may be multiple MAC addresses listed because we are using two network adapters. To determine which MAC address belongs to the networking adapter we are interested in, we need to look at the Advanced Settings of our VM network configuration.

To access the Advanced Settings, click on "Machine and settings" in the VM window, then click on the "Network" tab. Select the adapter we are interested in and expand the Advanced drop-down list to find the MAC address.

Once we have the MAC address, we can proceed to create the DHCP reservation on our DHCP server, which is ITF DC01. To do this, open the DHCP management console by opening the server manager and selecting "Tools" > "DHCP".

In the DHCP management console, expand our server, then expand the IP version 4 and our scope. Right-click on the reservations tab and choose "New Reservation".

In the new reservation dialog, enter the reservation name, which in this case is ITF WS001. Enter the IP address that we want the computer to receive, which is 192.168.0.134. Enter the MAC address that we obtained from the Windows 10 workstation. For the description, enter ITF workstation 0:01.

Leave the default checkbox for supported types checked. The bootp option, which stands for bootstrap protocol, is designed to dynamically assign IP addresses when computers boot up. Unlike DHCP, bootp can only configure the TCP/IP settings when a client computer is booted and not while it is already booted to Windows or while it's up and running at the desktop.

Click the "Add" button and then click "Close". Now, we can see the new reservation listed in the DHCP management console. Right-click on the new reservation to configure, delete, or edit its properties. Double-click on the reservation to see the settings for the router, DNS servers, and domain name. Note that these settings cannot be configured here, but can be changed by right-clicking on the reservation and selecting "Configure Options".

To test if the DHCP reservation is working, switch over to our Windows 10 VM and switch the IP configuration to DHCP. Login to the Windows 10 VM and click the Windows button. Search for "Network" and select "Network and Sharing Center". Select "Ethernet 2" and choose "Properties". Double-click on "IP version 4" and check the "Obtain an IP address automatically" and "Obtain DNS server address automatically" checkboxes. Click "OK" and close all the network windows.

Open the command prompt by pressing the Windows key and searching for CMD. Run the "ipconfig" command to check the IP configuration. Here, we can see that our Windows 10 VM has received the IP address that we reserved for it in DHCP.

Switch back over to our DHCP server and navigate to the address leases tab in the DHCP management console. Here, we can see that our workstation is listed, and under the lease expiration, it says "reservation active".

Congratulations! You have learned how to create a DHCP reservation. Great job!

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: CONFIGURING DHCP AND DNS ZONES IN WINDOWS SERVER
TOPIC: DNS ZONES IN WINDOWS SERVER

A DNS zone is a collection of DNS resource records that maps domain names to IP addresses. There are two main types of DNS zones: forward lookup zones and reverse lookup zones.

A forward lookup zone translates host names to IP addresses, while a reverse lookup zone does the opposite by translating an IP address to a hostname. For example, you can ask a DNS server for the IP address of a host name and it will respond with the corresponding IP address. Conversely, you can ask for the host name associated with a specific IP address.

Both forward and reverse lookup zones can contain primary, secondary, and stub zones.

A primary zone is a DNS zone for which the DNS server is the primary source of information. By default, the data for this zone is located in a file under the windows directory. It can also be stored in Active Directory if the DNS server is also a writable domain controller. Storing a primary zone in Active Directory allows for replication using the Active Directory replication process and provides additional security features. A primary zone is the only zone type that can be directly edited or updated.

A secondary zone is a read-only replica of a primary DNS zone hosted on another remote DNS server. It is not stored in Active Directory, as it is merely a copy of the primary zone. Any changes made to a secondary DNS zone will be passed on to the server hosting the primary DNS zone. The purpose of a secondary DNS zone is to provide redundancy in case the server hosting the primary copy becomes unavailable. However, replicating each record from one server to another can be resource-intensive in large networks with frequent DNS server changes.

A stub zone is similar to a secondary zone in that it is a read-only zone that obtains its information from another remote DNS server. The main difference is that a stub zone only contains information about authoritative nameservers, not resource records for computer names. This allows hosts on one network to obtain information from a DNS server on another network without the need for full data replication. A stub zone is a less resource-intensive alternative to a secondary zone.

Forward and reverse lookup zones are used to map domain names to IP addresses and vice versa. Primary zones are the primary source of information for a DNS server, while secondary zones provide redundancy. Stub zones contain information about authoritative nameservers and are used to obtain information from a DNS server on another network without full data replication.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: CONFIGURING DHCP AND DNS ZONES IN WINDOWS SERVER
TOPIC: CREATING A DNS ZONE

This part of the material is currently undergoing an update and will be republished shortly.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: RESOURCE RECORD TYPES

DNS servers play a crucial role in providing DNS-based data about computers on a network. Resource records are used to store this information, and in this didactic material, we will provide an overview of the most common types of resource records encountered while working on DNS.

The first type of resource record is the Start of Authority (SOA) record. Every zone contains an SOA record at the beginning, which holds information about the DNS server that provided the data for that specific zone.

The next resource record is the Name Server (NS) record. The NS record indicates the authoritative DNS servers for the zone. Every zone must have at least one NS record at the root of the zone.

The Address (A) record maps a Fully Qualified Domain Name (FQDN) to an IP address. It is used to associate a domain name with its corresponding IP address.

The Pointer (PTR) record performs the opposite function of an A record. It maps an IP address to a fully qualified domain name. It is useful for reverse DNS lookups.

The Canonical Name (CNAME) record creates an alias for a specified FQDN. It allows multiple domain names to be associated with a single IP address. For example, if the server's name was changed, a CNAME record could be created to redirect traffic from the old domain name to the new one.

The Mail Exchange (MX) record is used to specify email servers for the zone. It is used when there is a mail server, such as Exchange 2010, in the network.

The Service (SRV) record allows the specification of servers for a particular service or protocol. For example, if you are running a web server, you can create an SRV record to specify the FQDN and port of the server, making it easily accessible to anyone querying your DNS server.

Resource records in DNS servers provide essential information about computers on a network. Understanding the different types of resource records, such as SOA, NS, A, PTR, CNAME, MX, and SRV, is crucial for effective system administration in Windows Server.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: UNDERSTANDING ACTIVE DIRECTORY

Active Directory users and computers, also known as Active Directory or AD, is a tool that is installed when a server has the Active Directory domain services role installed. It is a live directory or database that stores user accounts and their passwords, computers, printers, file shares, security groups, and their respective permissions. Each of these objects is considered separate, but groups can contain other objects such as users, computers, printers, or file shares. Groups are often used for security purposes, allowing specific permissions to be assigned to objects within Active Directory using group policies.

One of the main purposes of Active Directory is to handle security authentication across the domain. It only allows authorized users to log on to the network, ensuring centralized security management of network resources. Usernames and passwords are stored in one location, eliminating the need for administrators to store this information on individual computers.

Common tasks in Active Directory include resetting user passwords and creating or deleting user accounts. For example, when a new employee is hired, their user account needs to be created, and they need assistance with logging in for the first time. Active Directory simplifies this process by storing all accounts in one place. Without Active Directory, a local account would need to be created on each computer the new employee needs to access. Additionally, when a password needs to be reset, it would need to be done on each computer the user has an account on. This becomes impractical when dealing with a large number of computers.

Active Directory solves this problem by having all accounts stored in one place. When a user tries to log into a domain joined workstation, the computer checks the entered credentials against the credentials stored in Active Directory. This means that when a user changes their password in Active Directory, the change is effective for all domain computers on the network. This applies not only to user accounts but also to other objects stored in Active Directory, such as computers, printers, file shares, and groups.

To access Active Directory, open Server Manager and click on Tools, then select Active Directory users and computers. The console will appear, with a navigation pane on the left and the contents of the current location on the right. The menu includes options to exit Active Directory, delete changes made to the view, and perform actions on selected objects. The action menu provides the same set of options that would appear when right-clicking on an object.

Understanding Active Directory is essential for system administrators managing Windows Server environments. It provides centralized security management and simplifies user account and password management across the network.

The View menu in Active Directory Users and Computers console allows administrators to customize their view by adding or removing columns to show or hide information. This can be particularly useful when trying to locate specific fields within a large number of objects in Active Directory. One important feature in this view is the advanced features mode, which displays hidden and useful information that may not be visible in the default view.

The Filter option in the View menu enables users to show or hide certain types of object types within the contents pane. This can be helpful when searching for specific object types, such as users or groups, within the same organizational unit that contains multiple object types.

The Customize option in the View menu allows further customization of the view within the Active Directory Users and Computers console. Users can show or hide different components, such as the description bar, console tree, standard menus, and standard toolbar. For most administrators, the default options work fine, so clicking OK is usually sufficient.

The Help menu provides quick access to help topics and the tech center website. It also allows users to view the version of the Microsoft Management Console (MMC) and Active Directory Users and Computers by clicking the "About" option for each respective item. This can be useful for troubleshooting or verifying the version of the software.

Below the menus, there are several action buttons. The navigational buttons allow users to navigate forwards or backwards, similar to using Windows Explorer. The buttons displayed will change depending on the selected object, and hovering over each button will display a tooltip explaining its function.

The toolbars section provides additional functionalities. Users can create new users, groups, or organizational units within the current container. Filtering options can also be set from this section, similar to using the "View" menu. Another important feature is the ability to search for different objects in Active Directory by clicking the "Define Objects in Active Directory" button. This feature allows users to search for users, contacts, groups, computers, printers, and file shares. The search can be narrowed down to a specific organizational unit or expanded to cover the entire directory.

On the left side of the console, the navigation pane displays saved queries and the name of the domain being serviced by Active Directory. Saved queries are often overlooked but can be valuable for quickly locating specific objects, such as expired or locked out user accounts, or accounts that have not logged in within the last 30 days. These searches can be saved for later use, making redundant tasks much easier. For example, a hiring manager may request a list of accounts that haven't logged in within the last 30 days to disable or delete them, and this can be accomplished using saved queries.

Lastly, right-clicking on the domain in the navigation pane allows users to perform several actions. Delegating control of the domain enables the selection of additional users who can manage the domain. The Find button provides a way to locate objects stored within the domain, similar to the search button in the toolbar.

In Windows Server administration, understanding Active Directory is crucial for managing network domains effectively. Active Directory is a centralized database that stores information about network resources, including users, computers, and other objects. In this didactic material, we will explore some important aspects of Active Directory administration.

To begin, let's discuss the option to change domains. This option is useful when you have a subdomain or another trusted domain on your network. Additionally, you can change to another domain controller using the "Change Domain Controller" button. However, if you only have one domain controller in your network, you won't be able to make this change.

Next, let's talk about the "Raise Domain Functional Level" button. This option enables Active Directory features when you have multiple domain controllers on a network that are not the same version. Some features are only available when all your servers are updated to the latest version. For example, if you have a Windows Server 2012 domain controller and a Windows Server 2016 domain controller servicing the same network, your domain's functional level would be that of the 2012 domain controller. This means that the service cannot use some of the new features introduced in Windows Server 2016. However, if you upgrade the 2012 server to 2016, you can raise the domain functional level to enable the new features.

Moving on, let's discuss the "Operations Masters" option. This allows you to choose which servers operate as master roles, such as the schema master, domain naming master, relative identifier master, primary domain controller emulator, and the infrastructure master. These roles are important for the proper functioning of Active Directory. When you remove a domain controller from the network, you may need to transfer these roles to another server. For example, if a domain controller holds the primary domain controller emulator (PDC) role and you want to remove it, you would first remove the role from that domain controller and transfer it to another server.

Active Directory domain services is a multi-master enabled database, which means that several domain controllers can make changes to this database. However, allowing multiple DCs to write changes to the database can sometimes cause conflicting updates. This is where operation masters step in to resolve the issue by only allowing certain DCs to make changes to certain parts of Active Directory domain services. It is important to have designated domain controllers for specific roles to avoid conflicting updates.

If you have only one domain controller on the network, you cannot change any of the operation master settings. Attempting to do so will result in an error message stating that the domain controller is the operations master. To transfer the operations master to another computer, you must first connect to it.

In addition to the above options, you can create new objects within Active Directory, such as user accounts, computer accounts, and more. The "All Tasks" option provides similar functionalities as the "View" option. You can also export lists of the domain's contents to a text file, refresh the view, access properties for various objects, and seek help if needed. While the built-in help documents can be useful, a quick search on Google often provides more practical guidance for specific tasks.

Understanding the administration options available in Active Directory is essential for effectively managing Windows Server domains. By utilizing these options, you can ensure the smooth operation of your network and optimize the use of Active Directory features.

Active Directory is a crucial component of Windows Server administration, providing a centralized and hierarchical database for managing network resources. It serves as a directory service, allowing administrators to efficiently control and organize user accounts, computers, and other network objects within a domain.

One of the primary benefits of Active Directory is its ability to provide a single sign-on experience for users. By authenticating against the domain controller, users can access various network resources without the need to remember multiple usernames and passwords. This simplifies the user experience and enhances security by enforcing strong password policies and access controls.

Active Directory utilizes a hierarchical structure, with domains serving as the fundamental organizational units. A domain represents a logical grouping of network objects and is administered by a domain controller. Multiple domains can be interconnected to form a domain tree, enabling centralized management and trust relationships between domains.

Within a domain, objects such as users, groups, and computers are stored in a directory database known as the Active Directory Domain Services (AD DS). This database stores information about each object, including attributes like usernames, passwords, email addresses, and group memberships.

Group Policy Objects (GPOs) are another essential feature of Active Directory. GPOs allow administrators to define and enforce security settings, software installations, and other configurations across multiple computers and users within a domain. This simplifies the management of large-scale deployments and ensures consistent security and configuration standards.

Active Directory also supports the concept of Organizational Units (OUs), which provide a way to further organize and delegate administrative tasks within a domain. OUs allow administrators to apply specific policies and permissions to different groups of objects, providing granular control over network management.

Active Directory is a powerful tool for system administrators, enabling centralized management of user accounts, computers, and other network resources. Its hierarchical structure, single sign-on capabilities, and support for Group Policy Objects make it an essential component of Windows Server administration.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: UNDERSTANDING ORGANIZATIONAL UNITS AND CONTAINERS IN WINDOWS SERVER

Organizational units (OUs) and containers are two important structural objects within Active Directory that serve different purposes. In this lesson, we will explore the differences between these two objects and understand their significance in Windows Server administration.

A container is a structural object that is included by default in Active Directory. It is important to note that group policy objects (GPOs) cannot be directly applied to containers. This limitation will become clearer when we discuss group policies later in this course. Additionally, it is not possible to create a container in Active Directory, although it can be done using ADSI Edit in certain scenarios, such as when launching new programs or management software suites like System Center Configuration Manager (SCCM).

By default, you will find several containers in Active Directory, including computers, foreign security principles, managed service accounts, and users. These containers can also be sorted by type, allowing you to group them together for easier management.

The computers container is the default location for new computers that join a domain. When a new workstation joins a domain, it is listed under this container by default. Although it is possible to change this default location using PowerShell, it is generally recommended to create a separate OU (organizational unit) for computers and apply GPOs there instead of the computers container. This allows for better organization and management of computers within the domain.

The foreign security principles container holds proxy objects for security principles from other trusted domains. A security principle from another domain can be a user account or a security group that resides in the other domain. This container is only used when a trust relationship is established between your domain and another. An example of when you would use this container is when you want to allow a user from another domain to be a part of the administrators group in your domain. In this case, you would add the proxy object representing the user from the other domain to your administrative group, and it would be stored inside the foreign security principles container.

The managed service accounts container holds accounts that are used to run services or applications on servers. These accounts, known as MSAs, are specifically designed for services and are not intended for use by end-users. Unlike regular user accounts, MSAs do not have passwords that need to be managed manually. Instead, the passwords for these accounts are handled automatically. This solves the problem of expiring service account passwords and enhances security for administrators. To create an MSA, you need to use the PowerShell command line, as there is currently no interface available for this purpose.

Within the users container, you will find the administrator and guest user accounts, along with several default security groups used by your domain. The users container also contains the built-in domain, which includes security groups required for the domain to operate. Examples of these groups include the administrator group, guest group, hyper-v administrators group, replicator group, and remote desktop users group.

It is important to note that the default security groups and built-in domain cannot be deleted, as they are essential for the proper functioning of your domain.

Understanding the differences between containers and organizational units is crucial for effective Windows Server administration. By utilizing OUs and properly organizing objects within Active Directory, administrators can apply appropriate group policies and enhance the overall management and security of their domain.

Organizational units (OUs) are an important aspect of Windows Server administration, specifically in the context of Active Directory. OUs are used to organize and separate objects within Active Directory, such as user accounts, computers, printers, and file shares. They provide a way to logically group related objects and apply specific permissions and policies to them.

By default, there is a pre-defined OU called "Domain Controllers" where computer objects are stored. This OU has a group policy object applied to it, which is a configuration that defines settings and restrictions for the objects within the OU.

Creating a new OU is a straightforward process. To do so, you need to right-click on the desired location within Active Directory, select "New," and then choose "Organizational Unit." A simple wizard will appear, allowing you to enter the name of the new OU. It is recommended to enable the option to protect the container from accidental deletion, unless you have specific intentions to delete it soon.

Once an OU is created, you can perform various actions on it. Right-clicking on an OU gives you options to cut, move, delete, rename, or refresh the OU. You can also create additional OUs within an existing OU, allowing for further organization and hierarchy.

It is crucial to place objects in the correct OU to ensure appropriate security privileges. Assigning permissions and policies to specific OUs allows system administrators to control access and settings for different groups of users or objects. Placing an object in the wrong OU can result in security vulnerabilities or access restrictions that are not intended.

Additionally, OUs provide the ability to export a list of objects within the OU. This can be useful for documentation or auditing purposes. However, it is important to note that the export list is not recursive, meaning it only includes objects within the selected OU and not any nested OUs.

Deleting an OU requires sufficient privileges and the object not being protected from accidental deletion. If an OU is protected, you need to disable the protection before deleting it. This can be done by accessing the OU properties and unchecking the "Protect container from accidental deletion" option.

Organizational units are a fundamental component of Windows Server administration and Active Directory. They allow for logical grouping and organization of objects, as well as the application of specific permissions and policies. Placing objects in the correct OU is crucial to ensure proper security and access control.

In this material, we will discuss organizational units (OUs) and containers in Windows Server. OUs and containers are used to organize and manage objects within Active Directory, such as users, groups, and computers.

To access the advanced features related to OUs and containers, follow these steps:
1. Open the Active Directory Users and Computers management console.
2. Navigate to the desired location within the directory structure.
3. Click on "View" in the menu bar and select "Advanced Features."

Enabling advanced features will display additional options for managing OUs and containers. Please note that all the previous options will still be available.

To modify the properties of an OU or container, right-click on it and select "Properties." In the "Object" tab, you can uncheck the "Protect object from accidental deletion" checkbox if you want to remove the protection. Click "OK" to save the changes.

To delete an OU or container, right-click on it and select "Delete." Confirm the deletion when prompted. Be aware that deleting an OU or container may also delete the objects it contains.

After making the necessary changes, you can turn off the advanced features by clicking on "View" and selecting "Advanced Features" again. This step is optional but can help declutter the management console.

By following these steps, you now have a clear understanding of what OUs and containers are, how to create new OUs, remove protection from accidental deletion, and delete OUs or containers.

Congratulations on completing this lesson! We hope you found it informative and look forward to seeing you in the next one.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: CREATING AND MANAGING USER ACCOUNTS

In this lesson, we will learn how to create and manage user accounts within Active Directory users and computers. This is a crucial skill for Windows server administrators and is essential for anyone looking to have a successful career in the IT field.

When it comes to creating and managing user accounts, there are two options available. The first option is to use the Active Directory users and computers console, while the second option is to use the PowerShell command line. However, most administrators prefer using the Active Directory users and computers console due to its graphical user interface and ease of use.

To access the Active Directory users and computers console, you can log in to your domain controller and select "Tools" and then "Active Directory users and computers" from the top right menu. Once opened, you will see the default organizational units and containers within your domain.

If you already have a structure set up in your workplace, you should follow that structure. However, if you are following along with this lesson, we will create our own structure. Let's assume we work for a company called "Eyeteeth Lee". We will create an organizational unit called "IT Fleet" by right-clicking on the root domain, selecting "New", and then "Organizational Unit". Inside the "IT Fleet" organizational unit, we will create two more organizational units: one for administrators and one for users. This will allow us to separate domain administrators from regular users.

Now, let's create a user account for ourselves under the administrators organizational unit. Right-click on the administrators organizational unit, select "New", and then "User". It is generally frowned upon in the security world to use shared user accounts, so it is better to create new user accounts for each individual. Fill in the necessary details such as first name, last name, and user logon name. The user logon name field has a separate logon for pre-Windows 2000 systems, which ensures compatibility with older server operating systems. Next, set up the user's password and confirm it.

Finally, it is important to note that the default administrator account should only be used as a backup and not for regular user accounts. Creating separate user accounts allows for better accountability and security.

Remember, the structure and organization of your Active Directory objects are entirely up to you and should be based on your specific needs and preferences.

When creating a new user account in Windows Server, the process typically involves creating the account in Active Directory with a temporary password. This temporary password is usually something like "password1" or any other simple combination. Once the account is created, the new user is provided with the username and temporary password. However, if we are creating the user account for ourselves, we can choose our own password and do not need to use a temporary one.

There are a few options to consider when creating a user account. The "User must change password at next logon" option allows the user to change their password when they first log in. If this option is unchecked, the user will not be prompted to change their password and will continue to use the password set during account creation.

Another option is the "User cannot change password" checkbox. When checked, it prevents the user from changing their password. This option is useful for service accounts that are not managed by an Active Directory domain.

The "Password never expires" checkbox is also available. If checked, the user's password will not expire. This option is commonly used for service accounts or for personal accounts when users do not want to change their password regularly.

Lastly, there is the "Account is disabled" checkbox. When checked, the account is created but disabled, making it unavailable for use until it is enabled. This option is useful when creating accounts in advance, such as for classroom environments where students will need access to computers on a specific date.

To create a user account, simply enter the desired password and configure the necessary options. It is important to note that enabling certain options, such as "User cannot change password" or "Password never expires," can impact the security of the account. Therefore, it is recommended to only enable these options when necessary.

Once the account is created, it can be modified to assign specific roles or permissions. For example, to make an account a domain administrator, the user can be added to the "Domain Admins" group. This can be done by accessing the account properties, navigating to the "Member Of" tab, clicking on the "Add" button, typing "Domain Admins," and confirming the selection.

Searching for user accounts or other objects within Active Directory can be done using the search feature. By clicking on the search button and selecting "Users, Contacts, and Groups," users can search for specific objects within the entire directory. This is particularly useful in larger organizations with multiple organizational units (OUs) and numerous users. By entering the name or other relevant details, users can quickly locate the desired account.

Creating and managing user accounts in Windows Server involves setting passwords, configuring options such as password change policies and account status, and assigning appropriate roles or permissions. Additionally, the search feature in Active Directory allows for easy retrieval of specific user accounts or other objects within the directory.

When it comes to system administration in Windows Server, creating and managing user accounts is a crucial task. In this lesson, we will explore the process of searching for users, unlocking their accounts, and resetting their passwords in Active Directory.

To search for a user, you can simply type in their name in the search bar. In most cases, this will be sufficient. However, there are other ways to search, such as using the employee ID. But for the majority of situations, typing in the user's name will be enough.

The primary reasons for searching for users are usually to unlock their accounts or reset their passwords. Resetting passwords in Active Directory is a straightforward process. Once you have found the user account you are looking for, you can right-click on it and choose "Reset Password."

When the reset password window appears, you will see options such as unlocking the account and requiring the user to change their password at the next logon. It's important to take note of the account lockout status on the domain controller. If the account is locked, you will need to check the corresponding checkbox.

You can then proceed to create a new password for the user, ensuring it meets the necessary complexity requirements. It is recommended to include a combination of alphanumeric characters and special symbols. Additionally, you should enable the option for the user to change their password at the next logon.

Once you have set the new password, click "OK" to save the changes. You can then provide the user with their new password. In case they are unsure about their username, you can double-click on their account and find the user logon name under the account tab.

Resetting passwords is a common task in domain controller administration, especially when dealing with a large number of users. It is an essential skill to possess for system administrators and helpdesk professionals.

Another aspect of managing user accounts is adding them to groups. In this lesson, we focused on the domain administrators group. By double-clicking on this group and navigating to the members tab, you can see the list of users who are part of this group.

To demonstrate the effects of a password reset, we logged in to the user account we had just reset the password for. Upon logging in, we were prompted to change the password, as indicated by the "user must change password at next logon" checkbox. We entered a new password, adhering to the complexity requirements, and successfully logged in.

This lesson covered the process of creating and managing user accounts in Windows Server. We explored searching for users, resetting passwords, and adding users to groups. These skills are essential for anyone working in the helpdesk or system administration fields.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: GROUPS AND MEMBERSHIPS

In this lesson, we will explore how to create groups and manage group memberships within Active Directory users and computers. We will also discuss the purpose of groups and how they can be utilized.

To begin, make sure you are logged into your domain controller and have the Active Directory users and computers console open.

First, we will create a new security group within the domain users organizational unit. Right-click on the desired organizational unit and select "New" followed by "Group". In the new group window, enter a group name, such as "Sales" (for example purposes). The pre-Windows 2000 name will be automatically populated.

Next, we need to understand the group scope and group type options. Under group scope, there are three options: domain local, global, and universal. The domain local scope is only usable within the domain it was created and cannot be accessed from another domain, even with a trust established. The global scope is similar to domain local, but can be accessed from another domain if a trust is established. The universal scope allows the group to be accessed by other forests that have established trust. For most cases, the global scope is recommended.

Under group type, there are two options: security and distribution. Security groups are used for authentication purposes, while distribution groups are used for email lists. For example, a security group can be used to grant access to specific folders and files, determine remote desktop permissions, etc. Distribution groups are used when an exchange server is set up on the network, allowing emails to be sent to all members of the group.

After selecting the appropriate group scope and group type, click OK to create the group.

To manage the group, right-click on the group and select "Properties". Here, you can add a description, email address, and modify the group's scope and type. The most important tabs are "Members" and "Member Of".

Under the "Members" tab, you can add individuals to the group by clicking the "Add" button, typing in their name, and clicking "Check Names" to verify the account. Once added, the individual becomes a member of the group.

The "Member Of" tab allows you to make the group a member of another group. Simply click "Add", enter the group name, and click "Check Names" to verify.

Remember to click "OK" to save any changes made to the group.

By utilizing groups and managing group memberships, you can effectively control access and permissions within your Windows Server environment.

In Windows Server administration, managing groups and memberships is an important aspect of system administration. By creating and managing groups, administrators can efficiently assign privileges and rights to multiple users simultaneously. This didactic material aims to provide a clear understanding of how groups and memberships work in Windows Server.

To begin, let's explore the concept of groups and their significance. A group is a collection of user accounts that share common characteristics or permissions. By assigning permissions to a group, administrators can easily manage access control and streamline the administration process.

In Windows Server, there are built-in groups that have predefined roles and permissions. One of these groups is the "Administrators" group, which has extensive privileges and rights. When a user is added to the Administrators group, they inherit all the privileges associated with it.

Now, let's delve into the process of managing groups and memberships. Using the Active Directory Users and Computers tool, administrators can create, modify, and delete groups. By right-clicking on the desired organizational unit (OU) and selecting "New" and then "Group," a new group can be created.

Once a group is created, administrators can add users to it. By selecting the group, going to the "Members" tab, and clicking "Add," users can be added from the Active Directory. This allows for efficient management of user privileges and permissions.

It is important to note that groups can also be members of other groups. This concept is known as group nesting. By adding a group to another group, all the members of the nested group inherit the permissions and privileges of the parent group. This hierarchical structure simplifies the management of user access and rights.

In the provided example, the Sales group is a member of the Administrators group. This means that any user added to the Sales group will also have the same privileges and rights as the Administrators group. By understanding group nesting, administrators can effectively assign permissions and manage user access within the Windows Server environment.

To remove a group, administrators can simply right-click on the group, select "Delete," and confirm the deletion. This process removes the group and any associated permissions or memberships.

Groups and memberships play a crucial role in Windows Server administration. By creating and managing groups, administrators can efficiently assign permissions and rights to multiple users. Group nesting allows for a hierarchical structure, simplifying the management of user access and privileges. Understanding these concepts is essential for effective system administration in Windows Server.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: SAVED QUERIES IN WINDOWS SERVER

In this lesson, we will learn how to create saved queries in Windows Server to simplify repetitive tasks. Saved queries allow us to easily list users who have not logged in within a specified time frame or identify locked out user accounts. These queries can be created using Active Directory in Windows Server.

To begin, make sure you are logged in to your domain controller and have Active Directory open. If you are not at this point, please pause the lesson and resume once you have Active Directory open.

To create a new query, right-click on "Saved Queries" and select "New" followed by "Query". A new query window will appear. In this window, you can enter a name and description for the query to help identify its purpose. For example, you can name the query "30 Days Since Last Logon" and provide a description such as "List of users who have not logged in within the last 30 days".

Next, you have the option to change the query scope by clicking on "Browse". This allows you to select a different domain or a specific organizational unit (OU) if desired. It is important to check the "Include sub containers" checkbox to ensure that the query searches within all OUs. If this checkbox is not selected, the query will not find any users stored within the selected OU.

Now, click on "Define Query" under the "Find" drop-down menu. Here, you will see various options such as users, contacts, groups, computers, printers, shared folders, organizational units, custom search, and common queries. For our first example, we will choose "Common Queries".

Under "Common Queries", select "Days Since Last Logon" from the drop-down menu and set the value to "30". This means the query will show user accounts that have not logged in within the last 30 days. Click "OK" to validate the query.

Please note that the query will not display the actual results immediately because the values need to be computed when the query is run. Time is constantly changing, so the query will dynamically update to show user accounts that meet the specified criteria.

Now, let's create another saved query to identify locked out user accounts. For this, we will use an advanced LDAP query.

Please note that the details of LDAP syntax are beyond the scope of this lesson. However, you can find more information about LDAP syntax in the resources section.

To create the advanced LDAP query, click on the "Find" drop-down menu and select "Advanced". Here, you can enter a specific LDAP query to search for locked out user accounts.

Once the query is created, you can easily access it in Active Directory and export the list if needed. This can be useful when your boss asks for a list of all users who haven't logged in within a specific time frame or when you need to identify locked out user accounts.

By utilizing saved queries in Windows Server, you can streamline your administrative tasks and retrieve valuable information quickly and efficiently.

In this lesson, we will explore the topic of saved queries in Windows Server administration. Saved queries are a powerful tool that allows system administrators to search for specific objects within Active Directory. While we will mainly focus on finding user accounts in this lesson, it's important to note that saved queries can be used to locate any object within Active Directory, such as printers, file shares, and more.

To create a new query, right-click on "Saved Queries" and select "New." Give your query a name, such as "Locked User Accounts." You can also provide a description, although this is optional. Next, click on "Define Query" and ensure that it is saved under the root IT fleet. Select "Find" and choose "Custom Search." Now, we need to start typing in the LDAP syntax.

The LDAP syntax for our query will consist of the object category, object class, and the parameter we want to search against, which in this case is the lockout time. We want to find user accounts with a lockout time greater than or equal to zero. To accomplish this, we will use the following syntax:

(objectCategory=person) AND (objectClass=user) AND (lockoutTime>=0)

By using parentheses and logical operators, we can specify the criteria for our search. The "objectCategory" is set to "person" because we are looking for user accounts. The "objectClass" is set to "user" since we are specifically searching for user accounts. The "lockoutTime" parameter is set to be greater than or equal to zero.

After defining the query, click "OK" to save it. You will see the query string displayed, along with some additional code. Don't worry about the extra code; it is automatically generated and not relevant to our query. Now, if there are any locked user accounts in the domain, they will be listed under "Locked User Accounts" in Active Directory.

To demonstrate this, you can intentionally lock a user account by entering an incorrect password multiple times. After three failed attempts, the account will be locked, and you will see it listed under "Locked User Accounts" in Active Directory. Please note that the number of failed login attempts before an account is locked can be configured in Group Policy.

If you receive a phone call from a user whose account is locked, you can easily find their account by searching for their username. Right-click on the query "Locked User Accounts" and select "Refresh" (or press F5) to update the list. From here, you can right-click on the locked account, reset the password, and choose to unlock the user account.

Additionally, if you need to provide a report of locked user accounts to your boss, you can export the list as a text file. Right-click on the query "Locked User Accounts," select "Export List," and save it to the desired location.

Remember, saved queries are not limited to user accounts. They can be used to locate any object within Active Directory. Feel free to explore and experiment with saved queries to find printers, file shares, or any other objects you need.

Saved queries in Windows Server administration are a valuable tool for system administrators. They allow for efficient searching and management of objects within Active Directory. By understanding the syntax and criteria for creating queries, you can easily locate specific objects, such as locked user accounts. Experiment with saved queries to expand your knowledge and enhance your system administration skills.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: GROUP POLICY

Group policy is a powerful tool used by system administrators to make configuration changes to users and computers in an Active Directory domain. It allows for the implementation of security configurations across the domain, such as restricting user access to certain computers or files, setting desktop backgrounds, and deploying software to workstations.

To understand group policy, it is important to have a solid understanding of Active Directory. Group policy works by applying Group Policy Objects (GPOs) to the organizational units (OUs) within Active Directory. A GPO contains configuration settings for both users and computers. When a GPO is applied to an OU, the settings configured in the GPO are applied to the users and computers within that OU.

GPOs can also be configured to only apply to certain objects by defining security filtering. The most common and default choice is the "authenticated users" group, which includes all valid users and computers within Active Directory. GPOs are applied recursively, meaning that the settings will also be applied to all sub-OUs beneath the original OU that the GPO was applied to.

To access group policy management, you need to open the server manager and select the "group policy management" tool. In the console, you will see a view of the forest, which includes domains, sites, group policy modeling, and group policy results. The domains folder contains all the domains within the forest, while the sites folder contains information about physical server locations. The group policy modeling and group policy results tools can be used for troubleshooting purposes.

Expanding the domains folder will show a similar view to that of Active Directory, displaying the OUs that have been created. Underneath the root domain, there is a default domain policy GPO that applies to all objects within the domain. This GPO also applies to all objects within the sub-OUs, such as IT fleet, administrators, and domain users.

The group policy objects folder contains all the GPOs within the domain, whether they are currently in use or not. Here, you can see the default domain policy and default domain controller policy. The latter applies specifically to domain controllers.

WMI filters allow for the addition of specific rules for when a GPO should be applied or not. For example, a GPO could be set to apply only if the computer is using Windows 7 or a newer operating system.

The starter GPOs folder is used for importing or exporting GPOs for distribution to other environments.

Group policy is a crucial tool for system administrators working with Windows Server. It allows for easy and efficient configuration changes across an Active Directory domain, ensuring consistent security settings and software deployments.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: CREATING AND MANAGING GROUP POLICY OBJECTS

Group Policy Objects (GPOs) are an important aspect of system administration in Windows Server. They contain settings and configurations that can be applied to users or computers stored in Active Directory. A domain can have multiple GPOs, and it is rare to find a domain with only one GPO. Additionally, a single GPO can be linked or applied to multiple users simultaneously.

To demonstrate this, let's take a look at an example. In the Group Policy Management console, we have two GPOs in our domain: the default domain policy and the default domain controllers policy. Suppose we want to link the default domain controllers policy to the "IT Fleet" organizational unit (OU). To do this, we can right-click on the OU, choose "Link an Existing GPO," and select the default domain controllers policy. Now, we can see that the GPO is applied to both the "IT Fleet" OU and the domain controllers OU.

Deleting a link is also possible. By right-clicking on the link and choosing "Delete," we can remove the link without deleting the GPO itself. After deleting the link, the GPO still remains in the domain.

GPOs are used in a modular sense, meaning that administrators can create multiple GPOs and apply them to OUs as needed. For example, a GPO can be created to install Flash Player on computers that require it, or a GPO can be created to prevent users from launching Internet Explorer. These GPOs can then be linked to the appropriate OUs.

Creating a GPO is similar to creating a user account or organizational unit in Active Directory. By right-clicking on the domain or OU, we can choose to create a GPO in the domain and link it. This allows us to create a new GPO and link it to the desired location.

Once a GPO is created, we can perform various actions on it. We can edit the GPO, enforce it to take precedence over other GPOs, enable or disable the link, and save a report of the GPO's configuration settings. The report provides a detailed overview of the GPO's settings, similar to clicking on the GPO and viewing its settings directly.

Additionally, we can customize the view of the GPOs, change columns, and adjust reporting settings. It is also possible to create a new view, although this is rarely necessary. Deleting the link, renaming the GPO, refreshing changes, and accessing help are other available options.

Group Policy Objects (GPOs) are essential for system administration in Windows Server. They contain settings and configurations that can be applied to users or computers in Active Directory. GPOs can be linked or applied to multiple users simultaneously, and they are used in a modular sense, allowing administrators to create and apply multiple GPOs as needed. Creating and managing GPOs is done through the Group Policy Management console, where various actions can be performed on the GPOs.

When working with Windows Server and managing Group Policy Objects (GPOs), it is important to understand the various configurations and settings that can be applied. In this didactic material, we will cover the basics of creating and managing GPOs, as well as the differences between computer and user configurations.

To begin, it is worth noting that while help files can provide some guidance, they may not always have the specific information you need. In such cases, turning to external resources like Google can be helpful in finding solutions to your queries.

To create a GPO, you can right-click on the desired location and select "Create a GPO in this domain, and link it here." This will create a new GPO that can be edited to configure settings. To edit a GPO, simply right-click on it and choose "Edit." This will open the Group Policy Editor, where you can make configuration changes.

Within the Group Policy Editor, you will find two types of configurations: computer and user. It is crucial to understand the distinction between these two configurations. Computer configurations will only be applied to computer objects, while user configurations will only be applied to user objects within Active Directory.

For example, if you apply a GPO to an OU that only contains computers and make changes under the user configuration, those settings will not be applied to the computer objects. The same applies if you apply a GPO to an OU that only contains users and make changes under the computer configuration.

Therefore, it is essential to carefully consider the objects within the OU where the GPO will be applied and make configuration changes accordingly. This understanding is crucial to avoid potential issues and ensure that the desired settings are applied correctly.

When it comes to deleting GPOs, it is important to note that deleting a link will only remove the link itself, not the GPO. To delete a GPO, right-click on it and choose "Delete." A prompt will appear asking if you want to delete the GPO and all links to it in the domain. Confirming this action will delete the GPO and its associated links within the domain.

It is worth mentioning that this deletion does not affect links in other domains, if any exist. Therefore, it is important to exercise caution when deleting GPOs and ensure that you are deleting the correct GPO.

This didactic material has covered the basics of creating and managing Group Policy Objects in Windows Server. Understanding the differences between computer and user configurations is crucial when configuring GPOs. Additionally, it is important to be aware of the distinction between deleting a link and deleting a GPO itself.

There is much more to learn about group policy and group policy objects, and we look forward to exploring these topics further in future lessons.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: SYSTEM ADMINISTRATION IN WINDOWS SERVER
TOPIC: GROUP POLICY PRECEDENCE IN WINDOWS SERVER

Group Policy precedence is an important concept in Windows Server administration as it determines the order in which Group Policy Objects (GPOs) and their settings are applied. Understanding this order is crucial when dealing with multiple GPOs that configure the same setting, as it helps identify which settings will be applied and which ones will be ignored.

The order in which group policy runs is as follows:

1. Local Group Policy: The local group policy is the first to be applied to the computer. It can be edited by accessing the gpedit.msc file. This policy is considered the least important.

2. Site Group Policy: Any group policy objects assigned to the site are then applied. This policy overrides any conflicts found between the local and site group policies. For example, if a desktop wallpaper is configured in both the local and site group policies, the site policy will take precedence.

3. Domain Policy: Policies assigned to the domain are applied next, on top of the site and local settings.

4. Organizational Unit (OU): GPOs linked to a specific OU are applied next. This also applies to sub-OUs, where the GPO linked to the sub-OU takes precedence over those above it.

5. Enforced Group Policy Objects: GPOs that have been enforced by right-clicking and selecting the "enforce" option are applied last. If conflicting settings exist between the local and enforced GPOs, the enforced GPOs will take precedence.

To remember this order, you can use the acronym LSDoE, which stands for Local, Site, Domain, OU, and Enforced.

It's also important to consider the difference between computer and user configurations within a GPO. The computer configuration is applied first, followed by the user configuration. In case of conflicting settings, the user configuration will take precedence.

To illustrate this concept, consider a scenario where five GPOs are configuring the same wallpaper settings. Each GPO specifies a different desktop background. The order of precedence determines which GPO will win in this scenario.

In the example provided, the local policy sets the background to "udemy.jpg". However, a site policy is added later, configuring it to "Paul is cool.jpg". As the site policy comes after the local policy in the order of precedence, "Paul is cool.jpg" will take effect.

If a domain policy is then applied, specifying "IT fleet.jpg" as the background, it will overwrite both the local and site policies, taking precedence.

Organizational units can also affect precedence. If a GPO is assigned to the OU "domain computers" and configures "ITF logo.jpg" as the background, it will take precedence over all other GPOs. Similarly, if a sub-OU called "workstations" has a GPO assigned to it, configuring "basketball.jpg" as the background, it will take effect over all other GPOs.

Understanding group policy precedence is essential for managing conflicting settings in Windows Server administration. Knowing the order in which GPOs are applied and how they interact with each other helps ensure that the desired settings are enforced.

Group Policy precedence in Windows Server is an important concept to understand in system administration. It determines the order in which Group Policy Objects (GPOs) are applied and which GPO takes precedence over others.

The order of precedence is as follows: local, site, domain, organizational unit (OU), and enforced. The last GPO to be applied wins. This can be remembered using the acronym LSDOE, which stands for local, site, domain, OU, and enforced.

When a GPO is enforced, it takes precedence over all other GPOs. For example, if the domain policy is enforced, it will take precedence over all other GPOs. This means that any settings defined in the enforced GPO will be applied, overriding any conflicting settings in other GPOs.

Blocked inheritance is another concept to consider when working with GPOs. It allows you to block the inheritance of GPOs from parent OUs. This means that only GPOs inside the specific OU will apply, except for enforced GPOs that are above the OU. To block inheritance, simply right-click on the OU and choose "block inheritance."

In the scenario where inheritance is blocked, the default domain policy will not apply to the OU, but other GPOs within the OU will still apply. This allows for more granular control over GPO application.

To better understand GPO precedence, let's consider an example. Suppose we have the following GPOs: ITFlee.jpg linked to ITFlee.com, ITFLogo.jpg linked to the ITFLeo OU, and PaulIsCool.jpg linked to the Administrators OU. In this scenario, since we are going down to a sub OU, the PaulIsCool.jpg GPO will take precedence over the others.

Understanding Group Policy precedence in Windows Server is crucial for effective system administration. Remembering the acronym LSDOE (local, site, domain, OU, and enforced) can help you recall the order of precedence. Enforced GPOs take precedence over others, and blocked inheritance allows for selective application of GPOs within OUs.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH POWERSHELL
TOPIC: STORING USER INPUT INTO VARIABLES WITH POWERSHELL

Windows PowerShell is a powerful tool that can be used to create user accounts in Active Directory. To begin, you need to be logged in to a domain controller or a computer with the necessary features installed. If you are logged in to a domain controller, all prerequisites will be met.

To access Windows PowerShell, click on the "Tools" menu on Windows Server and select "PowerShell ISE". This will open the PowerShell Integrated Scripting Environment.

In PowerShell, you can write scripts by clicking on the "Script" dropdown. This allows you to write a series of commands, save them, execute them, and edit them later.

Before we start writing our script, it's important to understand the use of comments. Comments are lines of code that are not executed but provide information for the viewer to understand the code. To write a comment in PowerShell, use the shift and number 3 keys.

Now, let's focus on storing user input into variables. To store the user's first name into a variable, use the dollar sign ($) followed by the variable name. For example, we can create a variable called "first name".

To set the variable to a specific value, you can use the equals sign (=) and assign the value in quotation marks. Alternatively, you can prompt the user for input using the "read-host" command. This command asks the user to input their first name and stores it in the variable.

To add a prompt for the user, use the "-prompt" argument followed by a prompt message in quotation marks. For example, "Please enter your first name".

To output the user's information, use the "echo" command. You can create a sentence that includes the variable's value by concatenating it with other text using the plus sign (+).

You can run the script by clicking on the play button. The script will prompt the user to enter their first name, store it in the variable, and then output the information.

Remember to use comments to document your code and explain what each section does. This will help you understand the code later on when you need to make changes.

By using variables and user input, you can create dynamic scripts that can be reused and adapted for different scenarios.

To store user input into variables with PowerShell, we can use the "read-host" command. This command allows us to prompt the user for input and store it in a variable. For example, if we want to store the user's first name, we can create a variable called "first name" and use the "read-host" command to prompt the user to enter their first name. The input will then be stored in the "first name" variable.

To create the variable, we use the following syntax:

```
$first_name = read-host "Please enter your first name"
```

In this example, the user will see the prompt "Please enter your first name" and can type in their first name. The input will be stored in the "first_name" variable.

We can then use the value stored in the variable in our code. For example, we can display a message that includes the user's first name:

```
Write-Host "Your first name is $first_name"
```

This will display the message "Your first name is [user's first name]".

Similarly, we can store the user's last name and password using the same process. We create a variable for each and use the "read-host" command to prompt the user for input. We can then use the values stored in the variables in our code.

For example:

```
$last_name = read-host "Please enter your last name"
$password = read-host "Please enter your password"

Write-Host "Your full name is $first_name $last_name"
Write-Host "Your password is $password"
```

This will display the user's full name and password based on the input provided.

By using the "read-host" command, we can prompt the user for input and store it in variables. This allows us to collect and use user input in our PowerShell scripts.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH POWERSHELL
TOPIC: CREATING ACTIVE DIRECTORY USER ACCOUNTS WITH POWERSHELL - PART 1

To create an Active Directory user account using PowerShell, we need to follow a series of steps. First, we need to import the Active Directory module by using the command "import-module ActiveDirectory". It is important to note that if you are not on a domain controller or do not have the module installed, you will encounter an error at this point.

Next, we need to specify where the user account will be stored in Active Directory. If we do not provide this information, the account creation will fail. To do this, we create a variable called "ouPath" and set it to the desired Organizational Unit (OU) path. The OU path can be found by opening Server Manager, navigating to Active Directory Users and Computers, enabling the advanced view, and right-clicking on the desired OU to view its properties. The OU path is specified in the Distinguished Name attribute.

After specifying the OU path, we need to secure the password before passing it to Active Directory. This is done by creating a new variable called "securePassword" and setting it to the result of the "ConvertTo-SecureString" command. The password to be converted is the one entered earlier using the "Read-Host" command.

Finally, we are ready to create the user account using the "New-ADUser" command. This command requires several arguments to be specified. In this case, we need to provide the user's first name and last name as arguments. These values are stored in the variables "firstName" and "lastName" respectively.

By following these steps, we can successfully create an Active Directory user account using PowerShell.

To create an Active Directory user account using PowerShell, several steps need to be followed. First, we need to specify the required fields. The given name will be the first name, and the surname will be the last name. To create the username, we combine the first name and last name using the format "first name dot last name" in quotation marks.

Next, we need to specify the path where the user accounts should be created. This can be done by using the variable for the path that has already been determined.

To set the account password, we use the "-accountpassword" argument. However, it is important to note that using "password" is not secure. Instead, we should use "securepassword," which is a variable set earlier in the script.

There are two true/false settings that need to be set. First, we set "change password at logon" to true. This ensures that users are forced to change their password upon logging in for the first time. This is important to prevent unauthorized access using standardized passwords.

Second, we need to specify whether the account is enabled or not. By setting "-enabled" to true, we ensure that the account is enabled immediately after creation.

Once all the necessary details have been specified, the script can be run. It will prompt for the user's first name, last name, and password. The password must meet Active Directory's complexity requirements.

After running the script, the user's full name and password will be displayed. However, it is not recommended to output the password in clear text.

To verify the account creation, we can check Active Directory. The new user account will appear with the specified details, including the logon name, first name, and last name.

It is important to note that if any required information is not provided, an error will occur, preventing the creation of the user account.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH POWERSHELL
TOPIC: CREATING ACTIVE DIRECTORY USER ACCOUNTS WITH POWERSHELL - PART 2

In this didactic material, we will learn how to create multiple user accounts in Active Directory using PowerShell. By using a loop, we can automate the process and avoid the need to rerun the script multiple times.

To implement this, we will use a while loop. First, we need to create a variable called "exit" and set it to a value other than "Q". This variable will control the loop. At the end of the script, we will check if the user wants to exit the loop by setting the variable "exit" to "Q". If the user types "Q", the loop will break, and the script will end.

To implement this, we need to indent all the code inside the while loop for better readability. Additionally, we will set the variable "exit" to null at the beginning of the script.

To prompt the user to exit the loop, we can use the "Read-Host" cmdlet. The user will be asked to type "Q" to stop creating user accounts. If the user enters "Q", the variable "exit" will be set to "Q", breaking the loop.

To test the script, we can run it and enter the first name, last name, and a password for the user account. After creating the account, the script will display a message asking the user to type "Q" to stop creating user accounts. If the user presses Enter, the loop will continue, allowing the creation of additional accounts.

To check if the user accounts have been created, we can navigate to Active Directory and verify their presence.

To make the account creation process even faster, we can use a standardized password. By removing the "Read-Host" cmdlet and setting the password to a fixed value, we can quickly create multiple accounts without entering a password each time.

To save and execute the script, we can use the "Save As" option in the "File" menu. After saving the script, we can run it by right-clicking and selecting "Run with PowerShell." This allows us to create user accounts without manually entering the script each time.

PowerShell provides a powerful way to automate the creation of user accounts in Active Directory. By utilizing loops and standardized passwords, we can streamline the process and save time.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: WORKING WITH POWERSHELL
TOPIC: CREATING USERS ACCOUNTS FROM A CSV SPREADSHEET WITH POWERSHELL

In this lesson, we will learn how to create user accounts with PowerShell for Active Directory based on a CSV spreadsheet. This method can be used with any comma-separated value spreadsheet, not just Excel.

The CSV spreadsheet contains information about the users, such as their job title, office phone, email address, and the destination organizational unit (OU) where the user will be placed. Sometimes, you may receive a list like this from your boss, requesting new user accounts to be created and placed in the appropriate OUs within a specific timeframe. Manually creating user accounts for multiple users can be time-consuming, especially if you have a large number of users to create.

To make your life easier, you can script this process in PowerShell. Instead of saving the spreadsheet as an Excel file, save it as a CSV file. In Excel, go to File > Save As and choose "Comma Separated Values" or "Comma Delimited" as the file type.

In PowerShell, we will import the necessary modules for working with Active Directory by using the command "Import-Module ActiveDirectory".

Next, we will prompt the user to enter the file path of the CSV spreadsheet by using the command "Read-Host". The file path will be assigned to a variable called "FilePath".

Once we have the file path, we will import the CSV file into a variable called "Users" using the command "Import-Csv" followed by the file path.

Now, we can start creating user accounts based on the information in the CSV file. We will loop through each user in the "Users" variable and use the "New-ADUser" cmdlet to create a new user account in the appropriate OU. We will specify the necessary attributes for each user, such as first name, last name, job title, office, email address, description, and the organizational unit.

It is important to note that you may need to adjust the organizational unit based on your specific requirements. You can find the distinguished name of an OU by opening the Active Directory Users and Computers console, enabling advanced features, right-clicking on the OU, choosing "Properties", and going to the "Attribute Editor" tab. The distinguished name is the OU path that we will be using.

By scripting this process in PowerShell, you can save a significant amount of time and effort when creating user accounts in Active Directory. This is especially useful when dealing with a large number of users or when user accounts need to be created frequently.

To create user accounts from a CSV spreadsheet using PowerShell, follow these steps:

1. Import the CSV file into a variable called "users". This can be done by opening Windows Explorer and locating the CSV file, which is typically found in the "resources" section of the lecture material or provided as a link in the TechNet article. Right-click on the file and choose "edit" to confirm that it contains the desired user information. Then, type the path of the CSV file (e.g., C:\new_users.csv) when prompted.

2. Next, loop through each row of the CSV file using a "foreach" command. This will allow you to extract specific information from each row, such as first name, last name, and job title. By doing so, you can create a new user account for each row in the CSV file.

3. To begin the loop, specify the variable name for each user (e.g., "user") within the "foreach" command. This will iterate through each line of the CSV file.

4. Within the loop, you can gather the user's information by assigning variables to each column. For example, use "Fname" to store the first name, "Lname" to store the last name, and "Jtitle" to store the job title. To extract the information, use the format "user.column_name" (e.g., user.first_name).

5. Confirm that the information is correctly stored by echoing the variable values. For example, if you want to display the first names of all users, use the command "echo Fname" within the loop. This will output the first name for each user in the CSV file.

By following these steps, you can easily create user accounts from a CSV spreadsheet using PowerShell. Remember to customize the variable names and file paths based on your specific requirements.

To create user accounts from a CSV spreadsheet using PowerShell, we need to follow a step-by-step process. First, we need to ensure that the variables in the CSV file are wrapped in quotation marks if they contain spaces. This is necessary for proper syntax.

Next, we need to identify the columns in the CSV file that contain the necessary information for creating user accounts. In this case, we have the columns for first name, last name, job title, office phone, email address, description, and organizational unit.

We can retrieve the values for each column by using the syntax "variable = user.columnName". For example, to retrieve the office phone value, we use "office phone = user.office phone". We can also use the "echo" command to display the retrieved values.

Once we have retrieved all the necessary values, we can proceed to create the user accounts. We use the "new-aduser" command to create a new user account for each user in the CSV file. The required arguments for this command are the user's name, given name, surname, user principal name, path, account password, change password at logon, office phone number, description, and neighborhood.

To ensure accuracy, we can use tab completion while entering the command to avoid mistakes. It is important to note that the order in which the arguments are entered does not matter, as long as they are all included.

After creating the user accounts, we can use the "echo" command to display a message confirming the account creation, including the user's first name, last name, and organizational unit. This message can serve as a confirmation for each new user account created.

Lastly, if necessary, we can create a new password for each user. This can be done by prompting the administrator to enter a new password or by randomly generating passwords for each user.

By following these steps, we can successfully create user accounts from a CSV spreadsheet using PowerShell.

To create user accounts from a CSV spreadsheet using PowerShell, we will follow the steps outlined in this didactic material.

First, we need to set a secure password for the user accounts. We will use the following command:

```
$securePassword = ConvertTo-
SecureString -String "testpassword0!" -AsPlainText -Force
```

Next, we will save the code to the desktop. We can name the file "create_users_from_CSV.ps1".

To execute the code, we right-click on the file and select "Run with PowerShell".

The script will prompt us to enter the path to our CSV file. We can provide the path and press Enter.

Upon execution, the script will create user accounts based on the data in the CSV file. We can verify the creation of the accounts by refreshing the user list.

The new user accounts will have various details populated, such as email address, phone number, description, and username.

If you prefer not to write the script yourself, you can download it from the attached resources.

To further enhance the script, you can experiment with additional functionalities. For example, you can prompt the user to input a password before creating each account. Additionally, you can generate random passwords for the users within the for loop and output them in clear text.

To pause the script before it ends, you can add the command "pause" at the appropriate location.

You can also explore additional fields and add them to the script, such as employee ID, office, and other relevant information.

By experimenting with the script and exploring different fields, you will gain a better understanding of its functionality and its potential applications.

Although this lesson may be longer than usual, we hope you found the information useful and enjoyable. We look forward to creating more lessons like this in the future.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: DNS AND HOSTS IN WINDOWS SERVER
TOPIC: CREATING DNS RESOURCE RECORDS IN WINDOWS SERVER

In this lecture, we will learn how to create DNS resource records for both forward and reverse lookup zones in Windows Server. Let's start by creating a DNS resource record in a forward lookup zone.

To do this, we need to expand the desired zone by left-clicking on it and then right-click on the zone. From the options, choose "Other New Records." Here, we can select the type of resource record we want to create. For this example, let's choose a CNAME (Canonical Name) resource record.

Next, we need to provide the necessary information for the record. In the "Alias Name" field, enter "DC." The fully qualified domain name (FQDN) will be "ITF-DC01.ITFLEA.com." Alternatively, you can click the "Browse" button to locate the FQDN of the host you are looking for. This record will create an alias for a domain controller. Click "OK" to create the record.

Once the record is created, you can see it listed in the resource record type window. Right-click on the record to delete or edit its properties. Under the properties, you will find a security tab where you can specify who is allowed to edit the resource record. The default options are usually sufficient, but you can customize this if needed.

Now, let's create a reverse PTR (Pointer) resource record for the server "ITF-DC01.ITFLEA.com." Expand the "Reverse Lookup Zones" folder and select the appropriate zone for your subnet. Right-click on the subnet and choose "New Pointer" or PTR. Enter the IP address for the host and then enter the hostname, which is "ITF-DC01.ITFLEA.com." Click "OK" to create the pointer record.

To complete a forward lookup, we can search for our newly created resource record in the "mytest" zone. Right-click on your DNS server (e.g., "ITF-DC01") and select "Launch NSlookup." The alias we created was called "DC" in the "mytest" zone, so that's what we want to search for. We can see that the FQDN "ITF-DC01.ITFLEA.com" is associated with the alias "DC" in the search results.

Next, let's run a reverse lookup by searching for the hostname that holds the IP address "10.0.2.10." To do this, simply enter the IP address in the reverse lookup tool. The DNS server will show us the FQDN of the hostname that is associated with this IP address.

It's important to note that if we were using the command prompt instead of the NSlookup tool, we would need to prefix these commands with "nslookup." For example, instead of typing "10.0.2.10," we would need to type "nslookup 10.0.2.10."

Congratulations! You now know how to create a resource record in both a forward and reverse lookup zone in Windows Server. Great job getting through this lecture, and we look forward to seeing you in the next one.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: DNS AND HOSTS IN WINDOWS SERVER
TOPIC: UNDERSTANDING DOMAIN NAME SYSTEM IN WINDOWS SERVER

The Domain Name System (DNS) is a fundamental component of computer networks and the internet. It serves as a phone book, mapping domain names to their associated IP addresses. DNS allows users to enter website addresses, such as facebook.com, instead of memorizing the corresponding IP address. In this lecture, we will explore DNS and learn how to use the DNS Manager in Windows Server.

DNS servers maintain a directory of host names and their related IP addresses. Each domain typically has its own DNS server, similar to how there can be multiple phone books. Windows Server provides a DNS role that can be installed and managed. To access the DNS Manager, open the Server Manager and select "Tools" > "DNS". From here, you can manage the DNS server and connect to remote DNS servers by right-clicking on "DNS" and selecting "Connect to a DNS server".

The DNS Manager allows various administrative functions, such as configuring the server and its zones, removing stale records, updating server data files, clearing the DNS cache, launching nslookup (a name server lookup tool), starting or stopping the DNS server, and editing server properties.

Nslookup is a command-line tool that allows us to query DNS servers. By launching nslookup and searching for a domain, such as "ITF WS 001", we can obtain information about the server servicing our DNS requests, the fully qualified domain name of the workstation, and its IP address.

In case the DNS server is offline, nslookup will not be able to query the DNS server. However, once the DNS server is started again, we can resume querying it.

Within the DNS Manager interface, we can see various components, including forward lookup zones, reverse lookup zones, trust points (trust anchors), and conditional forwarders. Forward and reverse lookup zones will be explained in later lectures. Trust points allow DNS servers to validate DNS data from other servers, while conditional forwarders enable a DNS server to forward specific DNS queries to other servers.

DNS is a critical system that translates domain names into IP addresses. The DNS Manager in Windows Server provides a comprehensive interface for managing DNS servers and performing administrative tasks. Understanding DNS and its management is essential for effective server administration.

EITC/IS/WSA WINDOWS SERVER ADMINISTRATION DIDACTIC MATERIALS
LESSON: DNS AND HOSTS IN WINDOWS SERVER
TOPIC: THE HOSTS FILE IN WINDOWS SERVER

Before the use of DNS servers, Windows computers utilized a host file to associate IP addresses with easily memorable names. This was similar to mapping an IP address to a specific name, such as mapping an IP address to "ITflea.com". The host file still exists in Windows Server and can be accessed by following these steps:

1. Open Windows Explorer and navigate to the C:\Windows\System32\drivers\etc directory.
2. Look for a file called "hosts" in this directory. Note that this file has no extension.
3. To edit the host file, open a text editor with administrative rights. For example, you can use Notepad by clicking the Windows button and searching for "Notepad". Right-click on Notepad and choose "Run as administrator".
4. Drag the host file into the text editor to open it. By running Notepad as an administrator, you can view and make changes to the contents of the host file.
5. It is important to note that hackers commonly manipulate this file for DNS poisoning. DNS poisoning involves entering a different IP address for a widely used website, such as Facebook.com. This allows hackers to redirect users to a website that appears to be Facebook but actually steals usernames and passwords.

To understand how the host file works, let's create a test entry and map it to a loopback IP address. The loopback IP address is 127.0.0.1, which refers to the computer you are currently logged into. Follow these steps:

1. Open Command Prompt and attempt to ping the test entry by typing its name. Since the DNS server does not have a record of this entry and it is not in the host file, the ping will fail.
2. To create an entry for it in the host file, go back to Notepad and type the desired IP address (127.0.0.1) at the bottom of the file. Then, press the space bar and enter the DNS hostname for the test entry.
3. Save the host file and return to Command Prompt. Use the up arrow to select the previous command and press Enter to ping the test entry again.
4. This time, you will see that the ping attempt is successful, as it is now referencing the loopback IP address specified in the host file.

Remember that you can use any hostname or IP address in the host file. However, for this example, we used a name that is unlikely to conflict with existing entries on your network.

Lastly, if you want to remove the test entry, go back to Notepad, delete the corresponding line, save the file, and close Notepad. After doing so, if you try to ping the test entry again, Command Prompt will indicate that the host cannot be found.

It is crucial to understand that the host file only affects the local computer and has no impact on other computers within the network. Each computer only looks at its own host file and does not reference the host files of other computers.

Congratulations on learning about the hosts file and how it is used! Great job on completing this lecture.