Installing and Configuring DNS, DHCP, and Active Directory Roles in Windows Server 2019

Objective

This is a hand note manual aims to guide you through installing and configuring DNS, DHCP, and Active Directory roles on a Windows Server 2019 virtual machine. These roles are fundamental for managing networked environments, providing centralized control over device management, IP address allocation, and domain services.

Pre-Requisites

1. **Windows Server 2019 Standard VM**: Ensure you have two VMs:
    - **Windows Server 2019** - for practicing role setup.
    - **Windows Server 2019 AD** - for deploying final configurations.
2. **Virtual Machine Settings**: Configure the VM's network as **Host-only** to isolate it from the internet/local network.
3. **PowerShell**: You'll need basic knowledge of PowerShell for administrative tasks.

Installing DNS, DHCP and Active Directory roles

In this project you will learn how to install several common roles that a server provides on a network. You will learn how to install the following roles:

- **Domain Name Service (DNS)** – this is used to function as a central point to deal with lookup requests for accessing machines on the network or internet.
- **Domain Host Configuration Protocol** – this is used to configure all machines on the network with a unique IP address.
- **Active Directory** – provides central administration and control of all devices and objects on the network.

The project will cover the following activities:

1. Installing DHCP
2. Configuring DNS
    a. Configuring a Reverse Lookup Zone

3. Installing Active Directory
    a. Configuring Active Directory
4. Configuring PowerShell

you will need **two versions** of this virtual machine:

- One to allow you to practice on setting up roles (i.e., the new version of the virtual machine you have created) - **Windows Server 2019**
- and one with the necessary roles installed to complete the rest of the labs - **Windows Server 2019 AD**

Configuring the network

You do not really want the virtual machine to connect to the internet/your local network. To stop this, you will need to change the network settings for the virtual machine.

1. When you click on the virtual machine, you should see the "Devices" section. Look at the "Network Adapter" setting. This will currently say "NAT" which means it will use your network connection to access the LAN and Internet. This will need to be changed.

2. Click on the "Edit virtual machine settings" option.

3. On the "Virtual Machine Settings" dialogue, click on the "Network Adapter" option on the left. On the right-hand side, select the "Host-only: A private network shared with the host" option and click on "OK". The network adapter option should now change to "Host-only". Click on "OK" to close the "Virtual Machine Settings" dialogue.

Making a Clone of the virtual machine

1. Make sure your **"Windows Server 2019"** VM is powered off but selected. In VMWare Workstation, click on the "VM" menu option at the top of the window and select the "Manage" then "Clone" items.

2. The "Clone Virtual Machine Wizard" will show. Click on "Next".

3. The "Current state in the virtual machine" option should be selected. Press "Next".

4. Click on the "Create a full clone" option and press "Next".

5. In the "Virtual Machine name" box, change the name to **"Windows Server 2019 AD"** and modify the "Location" box so that the directory has the same name. Click on "Finish".

Making the Virtual Machine non-persistent

1. Click on the "Windows Server 2019" virtual machine.

2. Click on "Edit virtual machine settings".

3. Click on the "Hard Disk" option.

4. On the right-hand side, click on the “Advanced” button.
5. Click the “Independent” tick box, and then click on “Nonpersistent”. Then press “OK”. The “Hard disk” option should now have “(Nonpersistent)” show with the disk size.
6. Click on “OK”.

Note: this means the “Windows Server 2019” virtual machine will reset itself to the initial image – i.e., a clean install of Windows Server 2019 Standard. This means you can install roles and practice as much as you want, and it will reset itself once you power off the virtual machine so that you can do things again.

Installing DNS

1. Start the “*Windows Server 2019*” virtual machine.
2. Click on “*Start*”, open the “Windows System” menu, and select the “*Command Prompt*” option or start typing in CMD.
3. Type **ipconfig** and press enter. Check to see what the IP address is. Keep the command prompt window open.
4. Click on the network icon in the bottom right of the system tray.
5. Click on the “*Network and Internet settings*” link.
6. Click on the “*Change adapter options*” link.
7. Select “*Ethernet0*”, then from the “Organize” drop down menu select “p*roperties*”.
8. Highlight the “*Internet Protocol Version 4 (TCP/IPv4)*” option and click on “*properties*”.
9. Select “*Use the following IP address*” and enter the following information**:**
10. IP address: **192.168.1.1**
11. Subnet mask: **255.255.255.0**
12. Select “*Use the following DNS server addresses*” and enter **192.168.1.1** in to the “*Preferred DNS server*” box.
13. Click on the “*OK*” button.
14. Click on the “*OK*” button on “Ethernet0 Properties” window.
15. Click on the “*Close*” button on the “*Connection Properties*” window.
16. Click on the “*Close*” button on the “Network *Connection*” window.
17. Click on the “*Close*” button on the “Network *Status*” window.
18. Move back to the command prompt window.

19. Confirm that the IP address of the server has now changed.

20. Type **exit** into the command prompt and press enter.

21. Go back to the "*Dashboard*" window and close it. Start it again by clicking on the windows start button and start typing in "server Manager". Once it opens, in the dashboard window, click on the "Mange" dropdown menu and select "*Add roles and features*" option.

22. On the "*Dashboard*" window, if it has closed you can start it again by clicking on the Windows start button and start typing in "Server Manager". Once it opens, in the dashboard window, click on the "Mange" dropdown menu and select "*Add roles and features*" option.

23. On the "*Before you Begin*" setup window, click on the "*Next*" button.

24. Click on the "Role-based or feature-based installation" option and click "Next".

25. Click "Next" on the "Destination Server" window as your local server should be selected by default.

26. Click on the "DNS Server" option. On the "Add features required for DNS server" popup, click on "Add features".

27. On the "Select features" window, click on "Next". Keep pressing next through the different windows until you get to the "Confirm installation selections" window. You can click on the "Restart the destination server automatically if required" option for the VM to reboot once things have been installed. Then click on the "Install" button and then follow the instructions.

    Note: Now the DNS server has been installed but not configured. We will come back to this in the "Configuring DNS" section.

Installing DHCP

1. On the "*Dashboard*" window, click on the "Manage" dropdown menu and select "*Add Roles and features*" option.

2. On the "*Before you Begin*" setup window, click on the "*Next*" button.

3. Click on the "Role-based or feature-based installation" option and click "Next".

4. Click "Next" on the "Destination Server" window as your local server should be selected by default.

5. Click on the "DHCP Server" option. On the "Add features required for DHCP server" popup, click on "Add features".

6. Click on the "*Next*" button and keep pressing "Next" until you get to the "Confirm installation selections" window. Click on the "Restart the destination server automatically if required" box and then click on "Install".

7. Once the role has been installed, click on "Close".

Note: Now the DHCP server has been installed but not configured.

To configure the DHCP server we need to do more steps…

8. On the Dashboard window, you should now see "DHCP" showing on the left-hand side of the window. Click on "DHCP". This will then show a list of all servers that have DHCP on the right. Select the machine in the server list and right click and select the "DHCP manager" option. You can also get to this via the start bar and typing in "DHCP".

9. On the left of the window, double click on "DHCP", then double click on the server name. Highlight the "IPv4" option and right click and select the "New Scope…" option.

10. On the "New Scope Wizard" window, press "Next".

    Note: You can also add or modify DHCP scopes from the DHCP manager after the DHCP service has been installed.

11. Type **Daily Planet IP Range** into the "*Scope Name*" and "Description" boxes.

12. Type **192.168.1.10** in to the "*Starting IP address*" box.

13. Type **192.168.1.50** into the "*Ending IP address*" box. Now click on "Next".

14. In the "Add Exclusions and Delay" window, click on "Next". However, have a think about what you would use this option for.

15. On the "Lease Duration" window, leave it at "8 days". Think about what leases are for and why you might need this on a corporate network. Click on "Next".

16. On the "Configure DHCP Options" window, select "Yes, I want to configure these options now" and click on "Next".

17. Add "192.168.1.1" into the IP address and click on the "Add" button. Then click on "Next".

18. In the "Domain Name and DNS servers" window, enter "dailyplanet.com" into the "Parent Domain" box. In the "IP address" box, type in "192.168.1.10" and press "Add". It will eventually produce a warning that the DNS server is not available/valid but ignore this. This is because you have not fully configured and enabled your DNS server yet. Click on "Next".

19. On the "WINS Servers" window, click on "Next". Have a think about WINS is and why this is not wise to have any on the network.

20. On the "Activate Scope" window verify that the "Yes, I want to a*ctivate this scope now*" radio button is selected and click on "Next".

21. Click on “Finish” to complete the wizard.

<u>Note</u>: Once DHCP has been initially configured, you can go back and alter configuration details using the Server Manger and DHCP Server role. Alternatively, you can use the DHCP option within the Windows Administrative Tools menu.

Additionally, we have only configured DHCP for IPv4 addresses. Windows Server 2019 also provides a DHCPv6 service for configuring IPv6 addresses. Investigate the IPv6 functionality in your own time.

Configuring DNS

1. On the "*Server Manager*" window, select the "DNS" option on the left. This will then show a list of all servers that have DNS installed on the right. Select the machine in the server list and right click and select the "DNS manager" option. You can also get to this via the start bar and typing in "DNS".

2. On the left of the window, double click on "DNS", then double click on the server name.

   Note: We will first setup a DNS forward lookup zone.

3. Select and right-click on "*Forward Lookup Zones*", and then select "*New Zone*".

4. On the "*Welcome to the New Zone Wizard*" window, click on the "*Next*" button.

5. Verify that the "*Primary Zone*" option is selected and then click on "*Next*".

6. On the "*Zone Name*" setup window, type **dailyplanet.com** into the "*Zone Name*" box and click on "*Next*".

7. On the "*Zone File*" setup window, click on "*Next*".

8. Click on the "*Do not allow dynamic updates*" option.

   Note: For now, we are turning off dynamic DNS updates because you have not setup Active Directory which allows secure dynamic updates from clients.

9. Click on the "*Next*" button.

10. Click on "*Finish*".

11. Now double click on the "*dailyplanet.com*" option under the "*Forward Lookup Zones*" section in the server manager to see what has been added.

Configuring a reverse lookup zone.

1. Select and right-click on "*Reverse Lookup Zones*" and click on "*New Zone*".

2. On the "*Welcome to the New Zone Wizard*" setup window, click on "*Next*".

3. On the "*Zone Type*" window, select "*Primary Zone*" and clear the "*Store the zone in Active Directory*" (available only if the DNS server is also a domain controller) and then click on "*Next*".

4. Select the "*IPv4 Reverse lookup zone*" option and click on "*Next*".

5. On the "*Reverse Lookup Zone Name*" setup window enter the first three octets of the server IP address into the "*Network ID*" box.

6. Click on "*Next*".

7. On the "*Zone File*" setup window, click on "*Next*" to accept the default settings.

8. On the "*Dynamic Update*" setup window, click on "*Next*" to accept the default settings.

9. Click on "*Finish*".

10. Now double click on the "*1.168.192.in-addr.arpa*" option under the "*Reverse Lookup Zones*" section in the server manager to see what has been added.

11. **Now shut down the server. You have now successfully learnt how to install DHCP and DNS roles on a server. By shutting down the virtual machine it will reset back to a clean version of Windows Server 2019 ready for the next exercise or for additional practice.**

Installing Active Directory

Note: By the end of this exercise, you will have a working Active Directory server. This would be the initial starting image for the rest of the labs for this module. By doing it in the "Windows Server 2019" virtual machine, it will reset itself once you shut it down. What you should do is use this VM to practice on Active Directory and once you have followed the steps correctly, and to redo this using the second virtual machine that you have created called "Windows Server 2019 AD". Once that has been setup, you will then need to make the virtual machine *Nonpersistent* to practice further labs.

1. Double click on the VMWare icon and start the "*Windows Server 2019*" virtual machine again.

2. Click on the network icon in the bottom right of the system tray.

3. Click on the "*Network and Internet settings*" link.

4. Click on the "*Change adapter options*" link.

5. Select "*Ethernet0*", then from the "Organize" drop down menu select "p*roperties*".

6. Highlight the "*Internet Protocol Version 4 (TCP/IPv4)*" option and click on "*properties*".

7. Select "*Use the following IP address*" and enter the following information**:**

8. IP address: **192.168.1.1**

9. Subnet mask: **255.255.255.0**

10. Select "*Use the following DNS server addresses*" and enter **192.168.1.1** in to the "*Preferred DNS server*" box.

11. Click on the "*OK*" button.

12. Click on the "*OK*" button on "Ethernet0 Properties" window.

13. Click on the "*Close*" button on the "*Connection Properties*" window.

14. Click on the "*Close*" button on the "Network *Connection*" window.

15. Click on the "*Close*" button on the "Network *Status*" window.

16. Move back to the command prompt window.
17. Confirm that the IP address of the server has now changed.
18. Type **exit** into the command prompt and press enter.
19. On the "*Server Manager*" / "Dashboard" window, select the "Manage" dropdown menu and then select the "*Add Roles and features*" option.
20. On the "*Before you Begin*" setup window, click on the "*Next*" button.
21. Click on the "Role-based or feature-based installation" option and click "Next".
22. Click "Next" on the "Destination Server" window as your local server should be selected by default.
23. Click on the "Active Directory Domain Services" option. On the "Add features required for Active Directory Domain Services" popup, click on "Add features".
24. The "Active Directory Domain Services" option should now be ticked. Click on "Next".
25. On the "Select features" window, click on "Next".
26. On the "Active Directory Domain Services" window, look at the information about Azure Active Directory and investigate further. Click on "Next".
27. Click on the "Restart the destination server automatically if required" box and then click on "Install".
28. Once the role has been installed, click on "Close".

Note: Now the Active Directory has been installed but not configured.

To configure the Active Directory, we need to do more steps…

Configuring Active Directory

1. Return to the Dashboard window. You should now see "AD DS" showing on the left-hand side of the window. Click on "AD DS". This will then show a list of all servers that have Active Directory on the right. At the top of the "servers" section of the window, there will a warning in yellow saying "Configuration required for Active Directory Domain Services at…". Click on the "More" on the right-hand side.
2. In the "All servers task details and notifications" window, click on the "Promote this server to a domain…" option.

3. On the "*Deployment Configuration*" setup screen, select the "*Add a new forest*" option. In the "Root Domain Name" box, enter "dailyplanet.com". Click on "Next".

4. On the "Domain Controller Options" window, have a look at the options and investigate more about the other domain controller options. In the "DSRM" password boxes, type in "P@55w0rd" and confirm it.

5. Now there is no DNS server available, and you are adding a new forest to a domain which does not have a controller. At this point you would put in a DNS record to link the domain name and forest together, however, for now, you will not do this. Click on the "Next" button.

6. Click on the "Next" button on the "Additional Options" window. You can investigate what NetBIOS is and why it might be required in your own time.

7. Accept the defaults on the "Paths" window and click "Next".

8. On the "Review Options" window, click on "Next". There is a "View Script" button which allows you view what the PowerShell script would be to install these options. You can open this and see what it says. Click on the "Next" button.

9. On the "Prerequisites Check" window, none of the checks should fail. There might be warnings which in practice you would ensure are corrected first. If there are any failed checks, you would need to go back and correct them before proceeding any further. Click on the "Install" button.

7. The Virtual machine should reboot once the service has been installed. This could take several minutes while it re-configures itself. Log back into the "Administrator" account again to continue. Notice the difference to the logon screen.

Note: You will be using several features within active directory – creating different kinds of objects (e.g., computers and users) as well as a variety of other features in later labs.

Configuring PowerShell

Note: To administer a server using the PowerShell prompt (you will be using this extensively during the rest of the labs) you will need to configure it so that it provides access to all the commands to modify and control active directory. The default PowerShell prompt does not allow you access to these administrative commands unless explicitly tell it to do so.

1. Find and open a PowerShell window using the start button.

2. To get help on what each command does, you can use the Get-Help cmdlet.

3. Test to see what commands are available which relate to active directory. You will need to use the Get-Command cmdlet. First, find out what this command will do by using get-help.

4. Now type in Get-Command *-AD* and see what commands it finds.

5. Now test to see if any commands are found by typing in Get-Command *-GPO*

6. Note: the AD and GPO prefixes are shorthand for Active Directory and Group Policy Objects – you will learn about these and use them more in a couple of labs.

7. Close the power shell window.

8. Now add a new shortcut on the desktop that points to PowerShell (either by finding the power shell executable or typing the following... To enter the details into the shortcut directly, type in:

   %windir%\system32\WindowsPowerShell\v1.0\powershell.exe

   into the location box of the shortcut.

9. Try the icon to see if power shell works and then see if the commands are available. Once you have checked, close the power shell window.

Note: PowerShell can be expanded by including several modules when it starts. To access the active directory functionality, you will need to import modules that provide these commands.

10. Edit the icon on the desktop and add the following to the end of the target information:

    -noexit –command import-module ActiveDirectory, GroupPolicy

    Important: do not miss the space " " at the start.

11. Now try the icon again and notice if it starts up differently and then try steps 4 & 5 again.

    Note: When running PowerShell scripts that originate from trusted modules, PowerShell will execute them directly. However, when you start to write your own scripts or use ones from a third party (e.g., from the Web) PowerShell will usually block them from running as they are viewed as not being trusted. This is to stop untrusted scripts from harming the system in anyway. This execution policy will need to be changed.

12. Type in **get-help set-executionpolicy** and **make notes about the different execution policies available and why it is important.**

13. To set the execution you will need to use the *set-executionpolicy* command. Read the help associated to this command to work out what needs to be done (and which execution policy to use).
14. Now shutdown the server.

Remember: Once you have practiced the Active directory exercise, you will need to repeat it for the "Windows Server 2019 AD" virtual machine instead. This virtual machine will still remember the changes. Once you complete the Active Directory exercise (do not install DHCP or DNS), you will need to change the virtual machine so that it is nonpersistent to practice further labs. From this point onward, the rest of the labs will use the Windows Server 2019 AD machine.

Conclusion

This project a setup by step guide that provides a foundational Windows Server 2019 environment for managing a network's essential services. The configuration steps will allow you to practice and extend the setup for further administrative and network management tasks.

Fundamental info

https://www.univention.com/blog-en/2019/03/brief-introduction-dhcp-dns/

Contact Information

If you have any questions, feedback, or would like to connect, feel free to reach out to me:

- **LinkedIn: linkedin.com/in/r-rafi-cybersecurity**

Thank you for reviewing my project.