Install Active Directory

Introduction and/or Background

TX-Rig Company wants a scalable solution for single sign-on (SSO) for their company network.

Texas Rig, Inc.

Fueling The Future.

Objectives

In this project/lab the student will:

- Install Active Directory Domain Services to enable single sign-on.

Equipment/Supplies Needed

- VMWare Workstation Pro
- Windows Server 2019 ISO

Assignment

As a member of the Server Administration Team, you have been asked to enable single sign-on within the corporate network. To accomplish this, you will install Active Directory Domain Services.

Part 1: Preparation

1. Make sure your Windows 2019 Server Virtual Machine is installed and activated.

2. Your VM NIC in VMWare workstation should be set to “Host only”.
   a. If it is not, with your server powered off, select your server in the left pane, then select **VM** from the menu, then **Settings**. Select **Network Adapter**, then **Host Only** and click **OK** to save the changes

3. Start your virtual machine and login as Administrator.

4. Your server should have the following static IP Address:
   a. IP address = 172.17.3.10
   b. Subnet mask = 255.255.255.0

    c. Default gateway = (Leave it blank)
    d. DNS server = 172.17.3.10

5. (PrtScr#1 – Take a **screenshot** of your IP address configuration.)
6. Verify your computer name is **SRV19-Your Initials**, and change it, if needed. Right-click **Start** and select **Control Panel**. Select **System and Security** and then **System**. If your computer name is not correct, click **Change Settings** and then **Change** to change it. Once a server has been promoted to a Domain Controller (DC), you cannot change the name without demoting it back to a member server.

7. Make sure the system time and time zone are set correctly. It is more difficult to change these settings on a DC. Right-click on the Date and Time on the taskbar and select **Adjust date/time**. Make sure **Central Time US & Canada** is selected. Click **Change** to change the date/time. Close the **Settings** window.

8. Event Viewer Utility – Check your Windows log files to ensure your server is healthy before we start the installation of AD & DNS; do not continue if you have unresolved issues, resolve problems then continue. Hint: Go to Server Manager – Tools to find the Event Viewer

9. Review Server's built in local user and group account and create a user account before installing Active Directory. In Server Manager, select **Tools**, then **Computer Management**. Select **Local Users and Groups** in the left pane. Right Click **Users** to create a new user account for employee John Smith.

Part 2: Install Active Directory Domain Services

1. Log on to your server as Administrator.

2. On the Server Manager screen, click on the **Manage** drop down menu and select **Add Roles and Features**.

3. On the **Before you begin** screen, click **Next**.

4. On the **Select installation type** screen, leave **Role-based or feature-based installation** checked and click **Next**.

5. On the **Select destination server** screen, make sure your server is selected and click **Next**.

6. On the **Select Server Roles** screen, select **Active Directory Domain Services** and click **Next**.

7. A message box appears showing which features will be installed. Click **Add Features** and click **Next**.
8. On the **Select features** screen, click **Next**.

9. Click **Next** on the next screen.

10. On the **Confirm installation selections** screen, place a check in the box next to **Restart the destination server if required**. A pop-up message box appears asking you if you do indeed want to restart the server if necessary. Click **Yes**, then click **Install**.

11. An **Installation progress status** window will appear. Wait until this process is complete and then click **Close**.

12. After closing the **Installation progress status** window, you will notice a yellow exclamation at the top right of the screen. Clicking on this icon will present you with a message box with the option to promote this server to a domain controller. Click on **Promote this server to a domain controller**.

13. On the **Deployment Configuration** screen, select **Add a new forest** and in the **Root domain name**: text box, type **TxRig-Your Initials.local**, then click **Ne**xt. NOTE: This may take a few minutes to process.

14. On the **Domain Controller Options** screen, make sure the **Forest functional level** and the **Domain functional lev**el are **BOTH** set to **Windows Server 2016**.

15. Type **Itnw1354** in the **Password** and **Confirm password** text boxes and click **Next**.

16. On the **DNS Options** screen, you will be presented with a warning message stating that a delegation for this DNS server cannot be created. This is normal for the 1st domain controller of your forest. Click **Next**.

17. On the **Additional Options** screen, after a few moments, the NetBIOS domain name will appear. (Q#1. Record the NetBIOS name.) Click **Next**.

18. On the **Paths** screen, you can choose locations for the database folder, log files, and SYSVOL folder. Specifying different physical disks for the database and log files can improve performance, but leave the defaults for now. (Q#2. Record the folder locations for the Database, Logs, and SYSVOL.) Click **Next**.

19. On the **Review Options** screen, you can review your choices and go back and make changes if necessary. You can also view the PowerShell script that is automatically created. (PrtScr#2 – Take a **screenshot** of the powershell script.) This is useful for installing AD DS on a server core server. Click **Next**.

20. On the **Prerequisites Check** screen, although you may see some warning signs, you should also see a green check box stating that all prerequisites checks passed successfully. If you see any red checks or x's, you will need to correct the errors. Click **Install.** This process may take a while to complete. Once complete, the server will restart.

Part 3: System Health – What Changed now that Active Directory is installed?

1. Login to your Server, open **Server Manager**, and select **Local Server**.

2. (PrtScr#3. Take a **screenshot** of your Computer name and Domain Name). Note: FQDN Entire name machine name + domain name Q#3. What is your new FQDN?____

3. Events – What type of messages exist for each of these areas: **Local Server, AD DS, and DNS**?

4. Summary / Overview or brief explanation– types of messages that exist – any critical errors – Explain. Q#4a Local Server, Q#4b AD DS, and Q#4c DNS.

Part 4: Administrative Tasks – User & Computer Management

1. In Server Manager, select **Tools** and then **Active Directory Users and Computers**.

2. Create yourself a user account. Under your domain, right click **Users,** select **New** and then **User**. Type in your First Name, Last Name, and User Name, then click **Next**. (Use the first letter of the first name and the last name for the username.) Type **Itnw1354** for your password and confirm it. Uncheck **User must change password at next logon** and click **Next**, then **Finish**. Note: Password Complexity – Domain Password Requirements must be more secure - Complexity requirements are enforced when passwords are changed or created.

3. By default, the minimum password length is 7 characters. Passwords must contain both alpha and numeric characters, preferably both upper and lower case. For this lab, use **Itnw1354** as your user password.

4. Add this newly created user to the Domain Admins Group.

5. PrtScr#4 & 5 Take a **screenshot** of this user object Account & Member Of tabs

6. Create a DNS Reverse Lookup Zone for your domain. In Server Manager, select **Tools** and then **DNS**. In the left pane, select your server, then **Forward Lookup Zones**, and click on the name of your domain. In the right pane, you see the records that the system created in the Forward Lookup Zone.

7. PrtScr#6 Take a **screenshot** of the records in the forward lookup zone

8. Setup the Reverse Lookup Zone. Right Click **Reverse Lookup Zones**, select **New Zone**, and click **Next**. Select **Primary Zone** and click **Next**. Select **To all DNS servers on domain controllers in this Domain** and click **Next**. Select **IPv4 Reverse Lookup Zone** and click **Next**. For Network ID, type **172.17.3** and click **Next**. Select **Allow only secure dynamic updates,** click **Next**, then **Finish**.

9. Add a PTR Record to the Reverse Lookup Zone. Select the **3.17.172.in-addr.arpa zone**, then right-click it, select **New Pointer PTR…**, type 172.17.3.10 for the host IP address, for the host name, click **Browse,** Select **server name,** click **OK,** Select **Forward Lookup zones,** click **OK,** select **your domain,** click **OK.** Select the **Host(A)** record for your server and click **OK**. Click **OK** on your **new resource record** to save it.

10. PrtScr#7 Take a **screenshot** of showing the PTR record in your reverse zone.

Congratulations, you have successfully installed Active Directory.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Take a screenshot of your IP Address Configuration (PrtScr#1) 10 points	
	Criteria #2: Record the NetBIOS Domain name (Q#1) 5 points	

	Criteria #3: Record the folder locations for the Database, Logs, and SYSVOL. (Q#2) 5 points	
	Criteria #4: Take a screenshot of the Powershell script. (PrtScr#2) 10 points	
	Criteria #5: Take a screenshot of your Computer name and Domain Name. (PrtScr#3) 10 points	
	Criteria #6: Record your new FQDN (Q#3) 5 points	
	Criteria #7: Local Server Event Log messages, if any. (Q#4a) 5 points	
	Criteria #8: AD DS Event log messages, if any (Q#4b) 5 points	
	Criteria #9:DNS Event Log Messages, If any (Q#4c) 5 points	
	Criteria #10:Take a screenshot of this user object Account & Member Of tabs (PrtScr#4&5) 20 points - 10 each	
	Criteria #11:Take a screenshot of the records in the forward lookup zone (PrtScr#6) 10 points	
	Criteria #12:Take a screenshot showing the PTR record in your reverse zone. (PrtScr#7) 10 points	