LABS

You are an IT administrator for Contoso tasked with deploying a new domain controller using Windows Server Core and managing Group Policies for the organization. Your responsibilities include installing and promoting the server as a domain controller, creating Organizational Units (OUs), managing user accounts and groups, and configuring Group Policy Objects (GPOs) to enforce security and operational standards. These tasks are essential for maintaining an organized and secure domain infrastructure.  
In this lab, you will deploy AD DS on a Server Core installation, create and manage AD DS objects, and configure GPOs to control registry access, screen saver timeout settings, and permissions for users and groups.

Deploying a domain controller on Server Core provides a lightweight, secure, and efficient solution for managing directory services. This exercise demonstrates how to install the AD DS role and promote a server to a domain controller.

|  |
| --- |
| 1. Connect to **SEA-ADM1** and, if needed, sign in as **CONTOSO\Administrator** with a password of **Pa55w.rd**. |
| 1. On **SEA-ADM1**, select **Start**, and then select **Windows PowerShell ISE** and run it as an administrator. |
| 1. To install the AD DS server role, at the Windows PowerShell command prompt, enter the following command, and then press Enter: 2. Install-WindowsFeature –Name AD-Domain-Services –ComputerName SEA-SVR1 |
| 1. To verify that the AD DS role is installed on **SEA-SVR1**, enter the following command, and then press Enter: 2. Get-WindowsFeature –ComputerName SEA-SVR1 |
| 1. In the output of the previous command, search for the **Active Directory Domain Services** checkbox, and then verify that it is selected. Then, search for **Remote Server Administration Tools**. Notice the **Role Administration Tools** node below it, and then verify that the **AD DS and AD LDS Tools** node is also selected. |

|  |
| --- |
| 1. Connect to **SEA-ADM1** and, if needed, sign in as **CONTOSO\Administrator** with a password of **Pa55w.rd**. |
| 1. On **SEA-ADM1**, select **Start**, and then select **Windows PowerShell ISE** and run it as an administrator. |
| 1. To install the AD DS server role, at the Windows PowerShell command prompt, enter the following command, and then press Enter: 2. Install-WindowsFeature –Name AD-Domain-Services –ComputerName SEA-SVR1 |
| 1. To verify that the AD DS role is installed on **SEA-SVR1**, enter the following command, and then press Enter: 2. Get-WindowsFeature –ComputerName SEA-SVR1 |
| 1. In the output of the previous command, search for the **Active Directory Domain Services** checkbox, and then verify that it is selected. Then, search for **Remote Server Administration Tools**. Notice the **Role Administration Tools** node below it, and then verify that the **AD DS and AD LDS Tools** node is also selected. |
|  |
| 1. Ensure that you are connected to the console session of SEA-ADM1. |
| 1. Switch to Windows PowerShell ISE (Admin). |
| 1. To create an Organizational Unit (OU) called Seattle in the Contoso AD DS domain, enter the following command, and then press Enter: 2. New-ADOrganizationalUnit -Name "Seattle" -Path "DC=contoso,DC=com" -ProtectedFromAccidentalDeletion $true -Server SEA-DC1.contoso.com |
| 1. To create a user account for Ty Carlson in the Seattle OU, enter the following command, and then press Enter: 2. New-ADUser -Name Ty -DisplayName 'Ty Carlson' -GivenName Ty -Surname Carlson -Path 'OU=Seattle,DC=contoso,DC=com' |
| 1. To set the password for the Ty's user account, enter the following command, and then press Enter: 2. Set-ADAccountPassword Ty |
| 1. When you receive a prompt for the current password, press Enter. |
| 1. When you receive a prompt for the desired password, enter Pa55w.rd, and then press Enter. |
| 1. When you receive a prompt to repeat the password, enter Pa55w.rd, and then press Enter. |
| 1. To enable the account, enter the following command, and then press Enter: 2. Enable-ADAccount Ty |
| 1. To create a domain global group named SeattleBranchUsers, enter the following command, and then press Enter:   New-ADGroup SeattleBranchUsers -Path 'OU=Seattle,DC=contoso,DC=com' -GroupScope Global -GroupCategory Security |
| 1. To add the Ty user account to the newly created group, enter the following command, and then press Enter:   Add-ADGroupMember -Identity SeattleBranchUsers -Members Ty |
| 1. To confirm that the user is in the group, enter the following command, and then press Enter:   Get-ADGroupMember -Identity SeattleBranchUsers |
| 1. To add the user to the local Administrators group, enter the following command, and then press Enter:   Add-LocalGroupMember -Group 'Administrators' -Member 'CONTOSO\Ty' |

Configuring Group Policy enables centralized management of user and computer settings, ensuring consistency and compliance with organizational standards. This exercise demonstrates how to create, edit, and link GPOs to enforce security and operational policies.

|  |
| --- |
| *Why Are You Doing This Task?*  *Creating and editing a GPO allows you to define settings, such as disabling registry access and configuring screen saver timeouts, to enforce security and operational policies across the domain.* |
| 1. On **SEA-ADM1**, from Server Manager, select **Tools**, and then select **Group Policy Management**. |
| 1. If necessary, switch to the **Group Policy Management** window. |
| 1. In the **Group Policy Management** console, in the navigation pane, expand **Forest:Contoso.com**, **Domains**, and **contoso.com**, and then select the **Group Policy Objects** container. |
| 1. In the navigation pane, right-click or access the context menu for the **Group Policy Objects** container, and then select **New**. |
| 1. In the **Name** text box, enter **CONTOSO Standards**, and then select **OK**. |
| 1. In the details pane, right-click or access the context menu for the **CONTOSO Standards** Group Policy Object (GPO), and then select **Edit**. |
| 1. In the **Group Policy Management Editor** window, in the navigation pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then select **System**. |
| 1. Double-click the **Prevent access to registry editing tools** policy setting or select the setting, and then press Enter. |
| 1. In the **Prevent access to registry editing tools** dialog box, select **Enabled**, and then select **OK**. |
| 1. In the navigation pane, expand **User** **Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then select **Personalization**. |
| 1. In the details pane, double-click or select the **Screen saver timeout** policy setting, and then press Enter. |
| 1. In the **Screen saver timeout** dialog box, select **Enabled**. In the **Seconds** text box, enter **600**, and then select **OK**. |
| 1. Double-click or select the **Password protect the screen saver** policy setting, and then press Enter. |
| 1. In the **Password protect the screen saver** dialog box, select **Enabled**, and then select **OK**. |
| 1. Close the **Group Policy Management Editor** window. |

|  |
| --- |
| *Why Are You Doing This Task?*  *Linking a GPO to an organizational unit ensures that the policy applies to the appropriate users and computers, enabling targeted management of settings.* |
| 1. In the **Group Policy Management** window, in the navigation pane, right-click or access the context menu for the contoso.com domain, and then select **Link an Existing GPO**. |
| 1. In the **Select GPO** dialog box, select **CONTOSO Standards**, and then select **OK**.   *Click the****Next****button below to proceed to the next page.* |

Exercise 2: Configuring Group Policy

|  |
| --- |
| ***Task 3:****Review the effects of the GPO's settings*  *Why Are You Doing This Task?*  *Reviewing the GPO’s effects helps confirm that the intended settings are applied correctly, ensuring that policies function as expected.* |
| 1. On **SEA-ADM1**, in the search box on the taskbar, enter **Control Panel**. |
| 1. In the **Best match** list, select **Control Panel**. |
| 1. Select **System and Security**, and then select **Allow an app through Windows Firewall**. |
| 1. In the **Allowed apps and features** list, locate the **Remote Event Log Management** entry, select the checkbox in the **Domain** column, and then select **OK**. |
| 1. Sign out, and then sign in as **CONTOSO\Ty** with the password **Pa55w.rd**. |
| 1. In the search box on the taskbar, enter **Control Panel**. |
| 1. In the **Best match** list, select **Control Panel**. |
| 1. In the search box in Control Panel, enter **screen saver**, and then select **Change screen saver**. (It might take a few minutes for the option to display.) |
| 1. In the **Screen Saver Settings** dialog box, notice that the **Wait** option is dimmed. You cannot change the time-out. Notice that the **On resume, display logon screen** option is selected and dimmed and that you cannot change the settings.   📝 **Note:** If the **On resume, display logon screen** option is not selected and dimmed, open a command prompt, run gpupdate /force, and repeat the preceding steps. |
| 1. Right-click or access the context menu for **Start**, and then select **Run**. |
| 1. In the **Run** dialog box, in the **Open** text box, enter **regedit**, and then select **OK**. Note the error message stating **Registry editing has been disabled by your administrator**. |
| 1. In the **Registry Editor** dialog box, select **OK**. |
| 1. Sign out and then sign in as **CONTOSO\Administrator** with the password **Pa55w.rd**. |
| Why Are You Doing This Task?  Creating and linking additional GPOs allows you to implement tailored settings for specific organizational units, ensuring that policies meet departmental needs. |
| 1. On SEA-ADM1, from Server Manager, select Tools, and then select Group Policy Management. |
| 1. If necessary, switch to the Group Policy Management window. |
| 1. In the Group Policy Management console, in the navigation pane, expand Forest: Contoso.com, Domains, and contoso.com, and then select Seattle. |
| 1. Right-click or access the context menu for the Seattle organizational unit (OU), and then select Create a GPO in this domain, and Link it here. |
| 1. In the New GPO dialog box, in the Name text box, enter Seattle Application Override, and then select OK. |
| 1. In the details pane, right-click or access the context menu for the Seattle Application Override GPO, and then select Edit. |
| 1. In the console tree, expand User Configuration, expand Policies, expand Administrative Templates, expand Control Panel, and then select Personalization. |
| 1. Double-click the Screen saver timeout policy setting or select the setting, and then press Enter. |
| 1. Select Disabled, and then select OK. |
| 1. Close the Group Policy Management Editor window. |

A screenshot of a computer

AI-generated content may be incorrect.

Exercise 2: Configuring Group Policy

|  |
| --- |
| ***Task 5 :****Verify the order of precedence*  *Why Are You Doing This Task?*  *Verifying the order of precedence ensures that settings from higher-priority GPOs override those from lower-priority ones, enabling effective conflict resolution.* |
| 1. Back in the **Group Policy Management Console** tree, ensure that the **Seattle** OU is selected. |
| 1. Select the **Group Policy Inheritance** tab and review its content.   📝 **Note:** The Seattle Application Override GPO has higher precedence than the CONTOSO Standards GPO. The screen saver time-out policy setting that you just configured in the Seattle Application Override GPO is applied after the setting in the CONTOSO Standards GPO. Therefore, the new setting will overwrite the CONTOSO Standards GPO setting. Screen saver time-out will be disabled for users within the scope of the Seattle Application Override GPO.  *Click the****Next****button below to* |

3. Exercise 2: Configuring Group Policy

|  |
| --- |
| ***Task 7:****Verify the application of settings*  *Why Are You Doing This Task?*  *Verifying the application of settings confirms that the GPOs are functioning as intended and that the expected outcomes are achieved, ensuring policy effectiveness.* |
| 1. In the navigation pane, in **Group Policy Management**, select **Group Policy Modeling**. |
| 1. Right-click or access the context menu for **Group Policy Modeling**, and then select **Group Policy Modeling Wizard**. |
| 1. In **Group Policy Modeling Wizard**, select **Next**. |
| 1. On the **Domain Controller Selection** page, accept the default settings, and then select **Next**. |
| 1. On the **User and Computer Selection** page, in the **User information** section, select **User**, and then, in the **User** text box, enter **CONTOSO\Ty** or use the **Browse** command button to locate the **Ty** user account. |
| 1. On the **User and Computer Selection** page, in the **Computer information** section, select **Computer**, and then, in the **Computer** text box, enter **CONTOSO\SEA-ADM1** or use the **Browse** command button to locate the **SEA-ADM1** computer. |
| 1. On the **User and Computer Selection** page, select **Next**. |
| 1. On the **Advanced Simulation Options** page, accept the default settings, and then select **Next**. |
| 1. On the **Alternate Active Directory Paths** page, note the user and computer locations, and then select **Next**. |
| 1. On the **User Security Groups** page, verify that the list of groups includes **CONTOSO\SeattleBranchUsers**, and then select **Next**. |
| 1. On the **Computer Security Groups** page, select **Next**. |
| 1. On the **WMI Filters for Users** page, accept the default settings, and then select **Next**. |
| 1. On the **WMI Filters for Computers** page, accept the default settings, and then select **Next**. |
| 1. On the **Summary of Selections** page, select **Next**. |
| 1. Select **Finish** when prompted. |
| 1. In the details pane, select the **Details** tab, and then select **show all**. |
| 1. In the report, scroll down until you locate the **User Details** section, and then locate the **Control Panel/Personalization** section. Note that the **Screen saver timeout** settings are **Disabled** and the **Winning GPO** is set to **Seattle Application Override** GPO. |
| 1. Close the **Group Policy Management** console. |