# Lab answer key: Implementing identity services and Group Policy

## Exercise 1: Deploying a new domain controller on Server Core

### Task 1: Deploy AD DS on a new Windows Server Core server

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Tools**, and then select **Windows PowerShell**.
3. At the command prompt in the Windows PowerShell command-line interface, enter the following command, and then select Enter:

powershell Install-WindowsFeature –Name AD-Domain-Services –ComputerName SEA-SVR1 1. Enter the following command to verify that the AD DS role is installed on **SEA-SVR1**, and then select Enter:

PowerShell Get-WindowsFeature –ComputerName SEA-SVR1 1. In the output of the previous command, search for **Active Directory Domain Services**. Verify that this check box is selected. Search for **Remote Server Administration Tools**. Notice the **Role Administration Tools** node below it, and then notice the **AD DS and AD LDS Tools** node.

**Note**: Under the **AD DS and AD LDS Tools** node, only **Active Directory module for Windows PowerShell** has been installed and not the graphical tools, such as the Active Directory Administrative Center. If you centrally manage your servers, you will not usually need these on each server. If you want to install them, you must specify the AD DS tools by running the **Add-WindowsFeature** cmdlet with the **RSAT-ADDS** command name.

**Note**: You might need to wait a brief time after the installation process completes before verifying that the AD DS role has installed. If you do not observe the expected results from the **Get-WindowsFeature** command, you can try again after a few minutes.

1. On **SEA-ADM1**, in **Server Manager**, select the **All Servers** view.
2. On the **Manage** menu, select **Add Servers**.
3. In the **Add Servers** dialog box, maintain the default settings, and then select **Find Now**.
4. In the **Active Directory** list of servers, select **SEA-SVR1**, select the arrow to add it to the **Selected** list, and then select **OK**.
5. On **SEA-ADM1**, ensure that the installation of the AD DS role on **SEA-SRV1** is complete and that the server was added to **Server Manager**. Then select the **Notifications** flag symbol.
6. Note the post-deployment configuration of **SEA-SVR1**, and then select the **Promote this server to a domain controller** link.
7. In the **Active Directory Domain Services Configuration Wizard**, on the **Deployment Configuration** page, under **Select the deployment operation**, verify that **Add a domain controller to an existing domain** is selected.
8. Ensure that the Contoso.com domain is specified, and then in the **Supply the credentials to perform this operation** section, select **Change**.
9. In the **Credentials for deployment operation** dialog box, in the **User name** box, enter \*\*Contoso\*, and then in the **Password** box, enter **Pa55w.rd**.
10. Select **OK**, and then select **Next**.
11. On the **Domain Controller Options** page, select the **Domain Name System (DNS) server** and **Global Catalog (GC)** check boxes. Ensure that the **Read-only domain controller (RODC)** check box is cleared.
12. In the **Type the Directory Services Restore Mode (DSRM) password** section, enter and confirm the password **Pa55w.rd**, and then select **Next**.
13. On the **DNS Options** page, select **Next**.
14. On the **Additional Options** page, select **Next**.
15. On the **Paths** page, keep the default path settings for the **Database** folder, **Log files** folder, and **SYSVOL** folder, and then select **Next**.
16. On the **Review Options** page, select **View script** to open the generated Windows PowerShell script.
17. In Notepad, edit the generated Windows PowerShell script:
    * Delete the comment lines that begin with the number sign (**#**).
    * Remove the **Import-Module** line.
    * Remove the grave accents (**`**) at the end of each line.
    * Remove the line breaks.
18. Now the **Install-ADDSDomainController** command and all the parameters are on one line. Place the cursor in front of the line, and then, on the menu, select **Select All** to select the whole line. On the menu, select **Edit**, and then select **Copy**.
19. Switch to the **Active Directory Domain Services Configuration Wizard**, and then select **Cancel**.
20. When prompted for confirmation, select **Yes** to cancel the wizard.
21. At the Windows PowerShell command prompt, enter the following command:

PowerShell Invoke-Command –ComputerName SEA-SVR1 { } 1. Place the cursor between the braces (**{ }**), and then paste the content of the copied script line from the clipboard. The whole line should now be as follows:

PowerShell Invoke-Command –ComputerName SEA-SVR1 {Install-ADDSDomainController -NoGlobalCatalog:\$false -CreateDnsDelegation:\$false -Credential (Get-Credential) -CriticalReplicationOnly:\$false -DatabasePath "C:\Windows\NTDS" -DomainName "Contoso.com" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:\$false -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:\$true} 1. Select Enter to start the command. 1. In the **Windows PowerShell Credential Request** dialog box, enter **Contoso\* in the** User name\*\* box, enter **Pa55w.rd** in the **Password** box, and then select **OK**. 1. When prompted for the password, in the **SafeModeAdministratorPassword** text box, enter **Pa55w.rd**, and then select Enter. 1. When prompted for confirmation, in the **Confirm SafeModeAdministratorPassword** text box, enter **Pa55w.rd**, and then select Enter. 1. Wait until the command runs and the **Status Success** message is returned. The **SEA-SVR1** virtual machine restarts. 1. Close Notepad without saving the file. 1. After **SEA-SVR1** restarts, on **SEA-ADM1**, switch to **Server Manager**, and on the left side, select the **AD DS** node. Note that **SEA-SVR1** has been added as a server and that the warning notification has disappeared.

**Note**: You might have to select **Refresh**.

## Task 2: Manage objects in AD DS

1. Switch to **SEA-ADM1**.
2. Switch to **Windows PowerShell (Admin)**.
3. Create an OU called **Seattle** in the domain by running the following command:

powershell New-ADOrganizationalUnit -Name:"Seattle" -Path:"DC=Contoso,DC=com" -ProtectedFromAccidentalDeletion:$true -Server:"SEA-DC1.Contoso.com"

1. Create a user account for **Ty Carlson** in the **Seattle** OU by running the following command:

powershell New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path "ou=Seattle,dc=contoso,dc=com"

1. Set the password for the account by running the following command:

powershell Set-ADAccountPassword Ty

1. When you receive a prompt for the current password, select Enter.
2. When you receive a prompt for the desired password, enter **Pa55w.rd**, and then select Enter.
3. When you receive a prompt to repeat the password, enter **Pa55w.rd**, and then select Enter.
4. To enable the account, run the following command:

powershell Enable-ADAccount Ty

1. Test the account by switching to **SEA-CL1**, and then sign in as **Ty** with the password **Pa55w.rd**.
2. On **SEA-ADM1**, in the **Administrator: Windows PowerShell** window, run the following command:

powershell New-ADGroup SeattleBranchUsers -Path "ou=Seattle,dc=contoso,dc=com" -GroupScope Global -GroupCategory Security

1. In the **Administrator: Windows PowerShell** window, run the following command:

powershell Add-ADGroupMember SeattleBranchUsers -Members Ty

1. Confirm that the user is in the group by running the following command:

powershell Get-ADGroupMember SeattleBranchUsers

**Results**: After this exercise, you should have successfully created a new domain controller and managed objects in AD DS.

## Exercise 2: Configuring Group Policy

### Task 1: Create and edit a GPO

1. On **SEA-ADM1**, from Server Manager, select **Tools**, and then select **Group Policy Management**.
2. If necessary, switch to the **Group Policy Management** window.
3. In **Group Policy Management Console**, on the **navigation** pane, expand **Forest:** Contoso.com, **Domains**, and Contoso.com, and then select the **Group Policy Objects** container.
4. On the **navigation** pane, right-click or access the context menu for the **Group Policy Objects** container, and then select **New**.
5. In the **Name** text box, enter **CONTOSO Standards**, and then select **OK**.
6. In the details pane, right-click or access the context menu for the **CONTOSO Standards** Group Policy Object (GPO), and then select **Edit**.
7. In the **Group Policy Management Editor** window, on the **navigation** pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then select **System**.
8. Double-click the **Prevent access to registry editing tools** policy setting or select the setting and then select Enter.
9. In the **Prevent access to registry editing tools** dialog box, select **Enabled**, and then select **OK**.
10. On the **navigation** pane, expand **User** **Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then select **Personalization**.
11. On the **details** pane, double-click or select the **Screen saver timeout** policy setting, and then select Enter.
12. In the **Screen saver timeout** dialog box, select **Enabled**. In the **Seconds** text box, enter **600**, and then select **OK**.
13. Double-click or select the **Password protect the screen saver** policy setting and then select Enter.
14. In the **Password protect the screen saver** dialog box, select **Enabled**, and then select **OK**.
15. Close the **Group Policy Management Editor** window.

### Task 2: Link the GPO

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**.
2. In the **Select GPO** dialog box, select **CONTOSO Standards**, and then select **OK**.

### Task 3: Review the effects of the GPO’s settings

1. Switch to **SEA-CL1**, and then sign in as **Contoso\* with the password** Pa55w.rd\*\*.
2. In the search box on the taskbar, enter **Control Panel**.
3. In the **Best match** list, select **Control Panel**.
4. Select **System and Security**, and then select **Allow an app through Windows Firewall**.
5. In the **Allowed apps and features** list, select the following check boxes, and then select **OK**:
   * **Remote Event Log Management**
   * **Windows Management Instrumentation (WMI)**
6. Sign out, and then sign in as **Contoso\* with the password** Pa55w.rd\*\*.
7. In the search box on the taskbar, enter **Control Panel**.
8. In the **Best match** list, select **Control Panel**.
9. 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.)
10. 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**.
2. In the **Run** dialog box, in the **Open** text box, enter **regedit**, and then select **OK**.
3. In the **Registry Editor** dialog box, select **OK**.

### Task 4: Create and link the required GPOs

1. On **SEA-ADM1**, in **Group Policy Management Console**, on the **navigation** pane, if necessary, expand **Forest:** Contoso.com, expand **Domains**, expand Contoso.com, and then select **Seattle**.
2. 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**.
3. In the **New GPO** dialog box, in the **Name** text box, enter **Seattle Application Override**, and then select **OK**.
4. On the **details** pane, right-click or access the context menu for the **Seattle Application Override** GPO, and then select **Edit**.
5. In the **console** tree, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then select **Personalization**.
6. Double-click the **Screen saver timeout** policy setting or select the setting and then select Enter.
7. Select **Disabled**, and then select **OK**.
8. Close the **Group Policy Management Editor** window.

### Task 5: Verify the order of precedence

1. In the **Group Policy Management Console** tree, select the **Seattle** OU.
2. Select the **Group Policy Inheritance** tab.

Notice that 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 standards setting and will prevail. Screen saver time-out will be unavailable for users within the scope of the Seattle Application Override GPO.

### Task 6: Configure the scope of a GPO with security filtering

1. On **SEA-ADM1**, in **Group Policy Management Console**, on the **navigation** pane, if necessary, expand the **Seattle** OU, and then select the **Seattle Application Override** GPO under the **Seattle** OU.
2. In the **Group Policy Management Console** dialog box, review the following message: "You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO, and will impact all other locations where this GPO is linked."
3. Select the **Do not show this message again** check box, and then select **OK**.
4. In the **Security Filtering** section, you will observe that the GPO applies by default to all authenticated users.
5. In the **Security Filtering** section, select **Authenticated Users**, and then select **Remove**.
6. In the **Group Policy Management** dialog box, select **OK**.
7. On the **details** pane, select **Add**.
8. In the **Select User, Computer, or Group** dialog box, in the **Enter the object name to select (examples):** text box, enter **SeattleBranchUsers**, and then select **OK**.
9. On the **details** pane, under **Security Filtering**, select **Add**.
10. In the **Select User, Computer, or Group** dialog box, select **Object Types**.
11. In the **Object Types** dialog box, select the **Computers** check box and then select **OK**.
12. In the **Select User, Computer, or Group** dialog box, in the **Enter Object Names to select (Examples)** text box, enter **SEA-CL1**, and then select **OK**.

**Note**: You may need to sign off and sign back on as Contosoon SEA-CL1 before preceding with the next step.

### Task 7: Verify the application of settings

1. In **Group Policy Management**, select **Group Policy Results** in the **navigation** pane.
2. Right-click or access the context menu for **Group Policy Results** and then select **Group Policy Results Wizard**.
3. In the **Group Policy Results Wizard**, select **Next**.
4. On the **Computer Selection** page, select **Another Computer**, and then enter **SEA-CL1** in the text box. Select **Next**.
5. On the **User Selection** page, in the list of users, select \*\*CONTOSO\*, and then select **Next**.
6. On the **Summary of Selections** page, select **Next**.
7. Select **Finish** when prompted.
8. On the **details** pane, select the **Details** tab, and then select **show all**.
9. In the report, scroll down until you locate the **User Details** section, and then locate the **Control Panel/Personalization** section. You should observe that the **Screen save timeout** settings are obtained from the Seattle Application Override GPO.
10. Close **Group Policy Management** console.

**Results**: After this exercise, you should have successfully created and configured GPOs.

## Exercise 3: Deploying and using certificate services

### Task 1: Create a new template based on the Web Server template

1. On **SEA-ADM1**, in **Server Manager**, select **Tools**, and then select **Certification Authority**.
2. In the **Microsoft Active Directory Certificate Services** dialog box, select **OK**.
3. In the **certsrv - [Certification Authority (Local)]** dialog box, right-click or access the context menu for the **Certification Authority (Local)** node, and then select **Retarget Certification Authority**.
4. In the **Certification Authority** dialog box, select **Another computer**, and then enter **SEA-DC1** and select **Finish**.
5. In the **Certification Authority** console, expand **ContosoCA**, right-click or access the context menu for **Certificate Templates**, and then select **Manage**.
6. In the **Certificate Templates Console**, locate the **Web Server** template in the list, select it, and then select **Duplicate Template**.
7. Select the **General** tab, in the **Template display name** text box, enter **Production Web Server**, and then enter **3** in the **Validity period** text box.
8. Select the **Request Handling** tab, select **Allow private key to be exported**, and then select **OK**. Minimize the **Certificate Templates** **Console**.
9. In the **Certification Authority** console on **SEA-ADM1**, right-click or select **Revoked Certificates**, select **All Tasks**, select **Publish**, and then select **OK** twice.

### Task 2: Configure templates so that they can be issued

1. On **SEA-ADM1**, in the **Certification Authority** console, right-click or access the context menu for **Certificate Templates**, point to **New**, and then select **Certificate Template to Issue**.
2. In the **Enable Certificate Templates** window, select **Production Web Server**, and then select **OK**.

### Task 3: Enroll the Web Server certificate on SEA-ADM1

1. Switch to **Windows PowerShell** and run the following command:

powershell Install-WindowsFeature Web-Server -IncludeManagementTools > **Note**: You may need to restart Certificate Services on **SEA-DC1** for the next step to work.

1. From **Server Manager**, select **Tools**, and then select **Internet Information Services (IIS) Manager**.
2. Select **SEA-ADM1**, and then in the central pane, double-click **Server Certificates** or select it and then select Enter.
3. In the **Actions** pane, select **Create Domain Certificate**.
4. On the **Distinguished Name Properties** page, complete the following fields, and then select **Next**:
   * Common name: sea-adm1.Contoso.com
   * Organization: **Contoso**
   * Organizational unit: **IT**
   * City/locality: **Seattle**
   * State/province: **WA**
   * Country/region: **US**
5. On the **Online Certification Authority** page, select **Select**, select **ContosoCA**, and then select **OK**.
6. In the **Friendly name** text box, enter **sea-adm1**, and then select **Finish**.
7. Ensure that the certificate displays in the **Server Certificates** console.
8. In the **IIS** console, expand **SEA-ADM1**, expand **Sites**, and then select **Default Web Site**.
9. In the **Actions** pane, select **Bindings**.
10. In the **Site Bindings** window, select **Add**.
11. In the **Add Site Binding** window, select **https** from the **Type** drop-down list. In the **SSL certificate** drop-down list, select **sea-adm1**, select **OK**, select **Yes**, and then select **Close**.
12. Close **Internet Information Services (IIS) Manager**.

**Results**: After completing this exercise, you should have configured certificate templates and managed certificates.

**Question**: During the lab, you collected data in a data collector set. What is the advantage of collecting data in this way?

**Answer**: You can review data in a data collector set periodically for comparative purposes.

©2019 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.