# Lab: Implementing identity services and Group Policy

## Scenario

You are working as an administrator at Contoso Ltd. The company is expanding its business with several new locations. The Active Directory Domain Services (AD DS) Administration team is currently evaluating methods available in Windows Server for rapid and remote domain controller deployment. The team is also searching for a way to automate certain AD DS administrative tasks. Additionally, the team wants to establish configuration management based on Group Policy Objects (GPO) and enterprise certification authority (CA) hierarchy.

## Objectives

After completing this lab, you’ll be able to:

* Deploy a new domain controller on Server Core.
* Configure Group Policy.
* Deploy, manage, and use digital certificates.

## Estimated time: 60 minutes

## Lab setup

Virtual machines: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR1**, **WS-011T00A-SEA-ADM1**, and **WS-011T00A-SEA-CL1**

User Name: **Contoso\Administrator**

Password: **Pa55w.rd**

## Lab setup

1. Select **SEA-DC1**.
2. Sign in using the following credentials:

* User name: **Administrator**
* Password: **Pa55w.rd**
* Domain: **Contoso**

1. Repeat these steps for **SEA-ADM1**, **SEA-SVR1**, and **SEA-CL1**.

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

### Scenario

As a part of business restructuring, Contoso wants to deploy new domain controllers in remote sites with minimal engagement of IT in remote locations. You need to use DC deployment to deploy new domain controllers.

The main tasks for this exercise are as follows:

1. Deploy AD DS on a new Windows Server Core server.
2. Manage AD DS objects with GUI tools and with Windows PowerShell.

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

1. Switch to **SEA-ADM1** and from **Server Manager**, open **Windows PowerShell**.
2. Use the **Install-WindowsFeature** cmdlet in Windows PowerShell to install the AD DS role on **SEA-SVR1**.
3. Use the **Get-WindowsFeature** cmdlet to verify the installation.
4. Ensure that you select the check boxes for **Active Directory Domain Services**, **Remote Server Administration Tools**, and **Role Administration Tools**. For the **AD DS** and **AD LDS Tools** nodes, only the **Active Directory module for Windows PowerShell** should be installed, and not the graphical tools, such as the Active Directory Administrative Center.

**Note**: If you centrally manage your servers, you will not usually need GUI tools on each server. If you want to install them, you need to specify the AD DS tools by running the **Add-WindowsFeature** cmdlet with the **RSAT-ADDS** command name.

**Note**: You might need to wait 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.

### Task 2: Prepare the AD DS installation and promote a remote server

1. On **SEA-ADM1**, from **Server Manager**, on the **All Servers** node, add **SEA-SVR1** as a managed server.
2. On **SEA-ADM1**, from **Server Manager**, configure **SEA-SVR1** as an AD DS domain controller by using the following settings:
   * Type: Additional domain controller for existing domain
   * Domain: Contoso.com
   * Credentials: **Contoso\* with the password** Pa55w.rd\*\*
   * Directory Services Restore Mode (DSRM) password: **Pa55w.rd**
   * Do not remove the selections for DNS and the global catalog
3. On the **Review Options** page, select **View Script**.
4. In Notepad, edit the generated Windows PowerShell script as follows:
   * Delete the comment lines, which begin with the number sign (#).
   * Remove the Import-Module line.
   * Remove the grave accents (`) at the end of each line.
   * Remove the line breaks.
5. Now that the **Install-ADDSDomainController** command and all the parameters are on one line, copy the command.
6. Switch to the **Active Directory Domain Services Configuration Wizard**, and then select **Cancel**.
7. Switch to **Windows PowerShell**, and then at the command prompt, enter the following command:

* Invoke-Command –ComputerName SEA-SVR1 { }

1. Paste the copied command between the braces ({ }), and then select Enter to start the installation. The complete command should 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. Provide the following credentials:
   * User name: \*\*Contoso\*
   * Password: **Pa55w.rd**
2. Enter and confirm the **SafeModeAdministratorPassword** as **Pa55w.rd**.
3. After **SEA-SVR1** restarts, on **SEA-ADM1**, switch to **Server Manager**, and then on the left side, select the **AD D** node. Note that **SEA-SVR1** has been added as a domain controller and that the warning notification has disappeared. You might have to select **Refresh**.

### Task 3: Manage objects in AD DS

1. Switch to **SEA-ADM1** and switch to Windows PowerShell.
2. Create an organizational unit (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. Run the following command to set the password as **Pa55w.rd**:

powershell Set-ADAccountPassword Ty > **Note**: The current password is blank.

1. Run the following command to enable the account:

powershell Enable-ADAccount Ty 1. Test the account by switching to **SEA-CL1**, and then sign in as **Ty** with the password **Pa55w.rd**. 1. 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

### Scenario

As a part of Group Policy implementation, you want to import custom administrative templates for Office apps and configure settings.

The main tasks for this exercise are as follows:

1. Create and edit GPO settings.
2. Apply and verify settings on the client computer.

#### Task 1: Create and edit a GPO

1. On **SEA-ADM1**, from **Server Manager**, open **Group Policy Management Console**.
2. Create a GPO named **Contoso Standards** in the **Group Policy Objects** container.
3. Edit the **Contoso Standards** policy, and then navigate to \*\*User ConfigurationTemplates\*.
4. Prevent users from accessing the registry by enabling the **Prevent access to registry editing tools** policy setting.
5. Navigate to the **User ConfigurationTemplatesPanel\* folder, and then configure the** Screen saver\*\* timeout policy to **600** seconds.
6. Enable the **Password protect the screen saver** policy setting, and then close the **Group Policy Management Editor** window.

#### Task 2: Link the GPO

* Link the **Contoso Standards** GPO to the Contoso.com domain.

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

1. Sign in to **SEA-CL1** as **Contoso\* with the password** Pa55w.rd\*\*.
2. Open **Control Panel**.
3. In **Windows Defender Firewall**, allow **Remote Event Log Management** and **Windows Management Instrumentation (WMI)** traffic.
4. Sign out and then sign in as **Contoso\* with the password** Pa55w.rd\*\*.
5. Attempt to change the screen saver wait time and resume settings. Group Policy prevents you from doing this.
6. Attempt to run Registry Editor. Group Policy prevents you from doing this.

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

1. On **SEA-ADM1**, in **Group Policy Management Console**, create a new GPO named **Seattle Application Override** that is linked to the **Seattle** OU.
2. Configure the **Screen saver timeout** policy setting to be disabled, and then 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 precedence over the Contoso Standards GPO. The screen saver time-out policy setting that you just configured in the Seattle Application Override GPO will be 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**, select the **Seattle Application Override** GPO. Notice that in the **Security Filtering** section, the GPO applies by default to all authenticated users.
2. In the **Security Filtering** section, remove **Authenticated Users**, add the **SeattleBranchUsers** group, and **SEA-CL1**.

**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. Launch the **Group Policy Results Wizard**.
3. Select the **SEA-CL1** computer and the \*\*CONTOSO\* user account.
4. After the report is created, in the details pane, select the **Details** tab, and then select **show all**.
5. In the report, scroll down until you locate the **User Details** section, and then locate the **Control Panel/Personalization** section. You should notice that the **Screen save timeout** settings are obtained from the Seattle Application Override GPO.

### Results

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

## Exercise 3: Deploying and using certificate services

### Scenario

Contoso has expanded; therefore, its security requirements also have increased. The security department is particularly interested in enabling secure access to critical websites and in providing additional security for some features. To address these and other security requirements, Contoso has decided to implement a public key infrastructure (PKI) by using the AD CS role in Windows Server. As a senior network administrator, you are responsible for implementing certificate enrollment. You also will be developing the procedures and process for managing certificate templates.

The main tasks for this exercise are as follows:

1. Create a new template based on the web server template.
2. Enroll the Web server certificate on **SEA-DC1**.

#### 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. Retarget the console to point to **SEA-DC1**.
3. In the **Certification Authority** console, open the **Certificate Templates Console**.
4. Duplicate the **Web Server template**.
5. Create a new template, and then name it **Production Web Server**.
6. Configure validity for **3** years.
7. Configure the private key as exportable.
8. Publish the CRL on **SEA-DC1**.

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

* Issue the certificates based on the **Production Web Server** template.

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

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

* Install-WindowsFeature Web-Server -IncludeManagementTools

1. Open **Server Manager**, and then open **Internet Information Services (IIS) Manager**.

**Note**: You may need to restart Certificate Services on **SEA-DC1** for the next step to work.

1. Enroll for a domain certificate by using the following settings:
   * Common name: sea-adm1.contoso.com
   * Organization: **Contoso**
   * Organizational unit: **IT**
   * City/locality: **Seattle**
   * State/province: **WA**
   * Country/region: **US**
   * Friendly name: **sea-adm1**
2. Create an HTTPS binding for the default website, and then associate it with the sea-adm1 certificate.

### Results

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

©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.