Contents

1 WS-011: Windows Server 2019 Administration

- **Download Latest Student Handbook and AllFiles Content**
- **Are you a MCT?** - Have a look at our GitHub User Guide for MCTs
- **Need to manually build the lab instructions?** - Instructions are available in the MicrosoftLearning/Docker-Build repository

1.1 What are we doing?

- To support this course, like other MOC courses, we are publishing the lab instructions and lab files on GitHub. However, unlike many of our other Azure courses, this Windows Server course doesn't use any Azure services, and so it's not subject to changes due to updates in the Azure platform. The files are provided on GitHub as a way to track things that need to be corrected. For typographical errors in the labs we will generally align those with changes made to the student handbook on a quarterly basis.

1.2 How should I use these files relative to the released MOC files?

- The instructor handbook and PowerPoints are still going to be your primary source for teaching the course content.
- These files on GitHub are designed to be used in conjunction with the student handbook, but are in GitHub as a central repository so MCTs and course authors can have a shared source for the latest lab files.

1.3 What about changes to the student handbook?

- We will review the student handbook on a quarterly basis and update through the normal MOC release channels as needed.

1.4 What can I do if I encounter errors in the lab instructions?

- Any MCT can submit a pull request to the code or content in the GitHub repo, Microsoft and the course author will triage and include content and lab code changes as needed.

1.5 Notes

1.5.1 Classroom Materials

1.6 It is strongly recommended that MCTs and Partners access these materials and in turn, provide them separately to students. Pointing students directly to GitHub to access Lab steps as part of an ongoing class will require them to access yet another UI as part of the course, contributing to a confusing experience for the student. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only.

1.7 title: Online Hosted Instructions permalink: index.html layout: home

2 Content Directory

Hyperlinks to each of the lab exercises and demos are listed below.

2.1 Labs

{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | | --- | --- | {% for activity in labs %}| {{ activity.lab.module }} | [{{ activity.lab.title }}{% if activity.lab.type %} - {{ activity.lab.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/WS-011-Windows-Server-2019-Administration/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 lab: title: 'Lab: Deploying and configuring Windows Server' module: 'Module 1: Windows Server administration'

3 Lab: Deploying and configuring Windows Server

3.1 Scenario

Contoso, Ltd. wants to implement several new servers in their environment, and they have decided to use Server Core. They also want to implement Windows Admin Center for remote management of both these servers and other servers in the organization.

3.2 Objectives

- Deploy and configure Server Core
- Implement and configure Windows Admin Center

3.3 Estimated time: 45 minutes

3.4 Lab setup

VMs: **WS-011T00A-SEA-DC1-B**, **WS-011T00A-SEA-ADM1-B**, **WS-011T00A-SEA-SVR4**

Username: **Contoso\Administrator**

Password: **Pa55w.rd**

For this lab, you'll use the available virtual machines, **WS-011T00A-SEA-DC1-B** and **WS-011T00A-SEA-ADM1-B**.

3.5 Exercise 1: Deploying and configuring Server Core

3.5.1 Scenario

As part of a deployment plan, you will implement Server Core and configure it for remote management. **WS-011T00A-SEA-SVR4-B** is pre-configured to open from the Win2019_1809_Eval.iso to install Windows Server.

The main tasks for this exercise are as follows:

1. Install Server Core.
2. Configure Server Core with sconfig and PowerShell.
3. Install Features on Demand on Server Core.

3.5.2 Task 1: Install Server Core

1. Start **WS-011T00A-SEA-SVR4-B**. Windows will start loading the installation files.
2. Install Windows Server 2019 Standard Evaluation.
3. Accept the license.
4. Perform a custom install.
5. Accept the default install location.
6. Set the Administrator password to **Pa55w.rd**.

3.5.3 Task 2: Configure Server Core with sconfig and PowerShell

1. At the command prompt, open the sconfig tool.
2. Access the Network Settings.
3. Modify adapter index #1.
4. Modify the following settings:
   - IP: **172.16.10.15**
   - Subnet mask: **255.255.0.0**
   - Default Gateway: **172.16.10.1**
5. Set the DNS server to be **172.16.10.10**. Leave the alternate DNS server blank.
6. Return to the main menu and exit to command line.
7. Open PowerShell.
8. Run the `Rename-Computer -NewName SEA-SVR4 -restart -force` cmdlet.
9. Sign in and open PowerShell
10. Run the `Add-Computer -DomainName Contoso.com -Credential Contoso\Administrator -restart -force` cmdlet. Enter **Pa55w.rd** when prompted for credentials.

3.5.4 Task 3: Install Features on Demand on Server Core

1. Mount the **Win2019_FOD.iso** image file to **drive D** of **SEA-SVR4**.
2. Sign in as **Contoso\Administrator**.
3. At the command prompt, run **Explorer.exe**. Note that command fails and returns an error.
4. Open PowerShell.
5. At the PowerShell prompt, run `Add-Windowscapability -Online -Name Servercore.Appcompatibility~~~~0.0.1. -Source D:`.
6. Run **Restart-computer**, and then sign in as **Administrator**.
7. Run **Explorer.exe**. Note that File Explorer now opens successfully.

3.5.5 Results

After completing this exercise, you will have installed Server Core, configured the networking settings, renamed the server, and joined the Contoso domain. You will have also installed Features on Demand.

3.6 Exercise 2: Implementing and using remote server administration

3.6.1 Scenario

Now that you have deployed the Server Core servers, you need to implement Windows Admin Center for remote administration.

The main tasks for this exercise are as follows:

1. Install Windows Admin Center.
2. Add servers for remote administration.

3. Configure Windows Admin Center extensions.
4. Verify remote administration.
5. Administer servers with Remote PowerShell.

3.6.2 Task 1: Install Windows Admin Center

1. Connect to **WS-011T00A-SEA-ADM1-B**.
2. Sign in as **Contoso\Administrator**.
3. Open File Explorer and browse to **C:\Labfiles\Mod01**.
4. Double-click or select **WindowsAdminCenter1910.2.msi**, and then select Enter. Install Windows Admen Center by accepting all the defaults.

3.6.3 Task 2: Add servers for remote administration

1. Open Microsoft Edge and go to `Https://Sea-Adm1`.
2. In Windows Admin Center, add **SEA-DC1** and **SEA-SVR4**.

3.6.4 Task 3: Configure Windows Admin Center extensions

1. Open **Settings**.
2. Select **Extensions**, and then select **Feeds**.
3. Add the package source **C:\Labfiles\Mod01**.
4. Select **Available Extensions**. Now you can observe the extensions.
5. Install the **DNS (Preview)** extension.
6. Switch to the Server Manager module.
7. Select **DNS** and install the DNS PowerShell tools. The tools will take a few moments to install.
8. Open the `Contoso.com` zone and observe the console.

3.6.5 Task 4: Verify remote administration

1. Select **Overview**. Note that the **details** pane contains basic server information performance monitoring much like **Task Manager**. In the left pane, observe the basic administration tools available.
2. Select **Roles and Features** and note what is installed and what is available to install.
3. Install the **Telnet Client**.
4. Open **Settings** and enable **Remote Desktop**.
5. Close the browser.

3.6.6 Task 5: Administer servers with Remote PowerShell

1. Open PowerShell.
2. Run the `Enter-PSSession -ComputerName SEA-DC1` cmdlet.
3. Run the `Get-Service -Name AppIDSvc` cmdlet. Note that the service is currently stopped.
4. Run the `Start-Service -Name AppIDSvc` cmdlet.
5. Run the `Get-Service -Name AppIDSvc` cmdlet. The service is running now.

3.6.7 Results

3.7 After completing this exercise, you will have installed Windows Admin Center and connected the server to manage. You performed management tasks of installing a feature and enabling Remote Desktop. Finally, you used Remote PowerShell to check the status of a service and start a service.

3.8 lab: title: 'Lab: Implementing identity services and Group Policy' module: 'Module 2: Identity services in Windows Server'

4 Lab: Implementing identity services and Group Policy

4.1 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.

4.2 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.

4.3 Estimated time: 60 minutes

4.4 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**

4.5 Lab setup

1. Select **SEA-DC1**.
2. Sign in using the following credentials:
   - User name: **Administrator**
   - Password: **Pa55w.rd**
   - Domain: **Contoso**
3. Repeat these steps for **SEA-ADM1**, **SEA-SVR1**, and **SEA-CL1**.

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

4.6.1 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.

4.6.2 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.

4.6.3 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\Administrator** 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 { }
   ```

8. Paste the copied command between the braces ({ }), and then select Enter to start the installation. The complete command should be as follows:

   ```
   Invoke-Command -ComputerName SEA-SVR1 {Install-ADDSDomainController -NoGlobalCatalog:\$false -Crea
   ```

9. Provide the following credentials:
   - User name: **Contoso\Administrator**
   - Password: **Pa55w.rd**
10. Enter and confirm the **SafeModeAdministratorPassword** as **Pa55w.rd**.
11. 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**.

4.6.4 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:

   ```
   New-ADOrganizationalUnit -Name:"Seattle" -Path:"DC=Contoso,DC=com" -ProtectedFromAccidentalDeletio
   ```

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

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

4. Run the following command to set the password as **Pa55w.rd**:

   ```
   Set-ADAccountPassword Ty
   ```

   Note: The current password is blank.

1. Run the following command to enable the account:

   ```
   Enable-ADAccount Ty
   ```

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

   ```
   New-ADGroup SeattleBranchUsers -Path "ou=Seattle,dc=contoso,dc=com" -GroupScope Global -GroupCateg
   ```

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

   ```
   Add-ADGroupMember SeattleBranchUsers -Members Ty
   ```

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

   ```
   Get-ADGroupMember SeattleBranchUsers
   ```

4.6.5 Results

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

4.7 Exercise 2: Configuring Group Policy

4.7.1 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.

4.7.1.1 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 Configuration\Policies\Administrative Templates\System**.
4. Prevent users from accessing the registry by enabling the **Prevent access to registry editing tools** policy setting.
5. Navigate to the **User Configuration\Policies\Administrative Templates\Control Panel\Personalization** 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.

4.7.1.2 Task 2: Link the GPO

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

4.7.1.3 Task 3: Review the effects of the GPO's settings

1. Sign in to **SEA-CL1** as **Contoso\Administrator** 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\Ty** 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.

4.7.1.4 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.

4.7.1.5 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.

4.7.1.6 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 Contoso\Ty on **SEA-CL1** before preceding with the next step.

4.7.1.7 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\Ty** 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.

4.7.2 Results

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

4.8 Exercise 3: Deploying and using certificate services

4.8.1 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**.

4.8.1.1 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**.

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

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

4.8.1.3 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.

2. 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**

3. Create an HTTPS binding for the default website, and then associate it with the sea-adm1 certificate.

4.8.2 Results

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

4.10 lab: title: 'Lab: Implementing and configuring network infrastructure services in Windows Server' module: 'Module 3: Network Infrastructure services in Windows Server'

5 Lab: Implementing and configuring network infrastructure services in Windows Server

5.1 Scenario

Contoso, Ltd. is a large organization with complex requirements for network services. To help meet these requirements, you will deploy and configure DHCP so that it is highly available to ensure service availability. You will also set up DNS so that Trey Research, a department within Contoso, can have its own DNS server in the testing area. Finally, you will provide remote access to Windows Admin Center and secure it with Web Application Proxy.

5.2 Objectives

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

- Deploy and configure DHCP
- Deploy and configure DNS

5.3 Estimated time: 30 minutes

5.4 Lab Setup

Virtual machines:

- **SEA-DC1**
- **SEA-ADM1**
- **SEA-SVR1**
- **SEA-CL1**

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

For this lab, you'll use the available virtual machine environment. Before you begin the lab, complete the following steps:

1. Open **SEA-DC1** and sign in as **Contoso\Administrator** with the password **Pa55w.rd**.

2. Repeat step 1 for **SEA-ADM1**, **SEA-SVR1**, and **SEA-CL1**.

5.5 Exercise 1: Deploying and configuring DHCP

5.5.1 Scenario

The Trey Research subdivision of Contoso, Ltd. has a separate office with only about 50 users. They have been manually configuring IP addresses on all of their computers and want to begin using DHCP instead. You will install DHCP on **SEA-SVR1** with a scope for the Trey Research site. Additionally, you will configure DHCP Failover by using the new DHCP server for high availability with **SEA-DC1**.

The main tasks for this exercise are as follows:

1. Install the DHCP role.
2. Authorize the DHCP server.
3. Create a scope.
4. Configure DHCP Failover.
5. Verify DHCP functionality.

5.5.2 Task 1: Install the DHCP role

1. On **SEA-ADM1**, open **Microsoft Edge**, and then sign in to **Windows Admin Center**.
2. In **Windows Admin Center**, connect to **SEA-SVR1**.
3. From **Roles & features**, install the DHCP role.
4. From **DHCP**, install the **DHCP PowerShell** tools. If **DHCP** is not available in the **Tools pane** for **SEA-SVR1**, close **Microsoft Edge** and sign in to **Windows Admin Center** again.

5.5.3 Task 2: Authorize the DHCP server

1. On **SEA-ADM1**, open **Server Manager**.
2. In **Server Manager**, open **Notifications**, open **Complete DHCP configuration**, and then complete the **DHCP Post-Install Configuration Wizard** by using the default options.

5.5.4 Task 3: Create a scope

1. On **SEA-ADM1**, in **Windows Admin Center**, while connected to **SEA-SVR1**, use **DHCP** to create a new scope with the following options:
   - Protocol: **IPv4**
   - Name: **ContosoClients**
   - Starting IP address: **10.100.150.50**
   - Ending IP address: **10.100.150.254**
   - DHCP client subnet mask: **255.255.255.0**
   - Router: **10.100.150.1**
   - Lease duration: **4 days**
2. In **Server Manager**, open the **DHCP management console**.
3. In the **DHCP management console**, add all authorized servers.
4. On the DHCP server **172.16.10.12**, in the **ContosoClients** scope, add the scope option **006 DNS Servers** with the value **172.16.10.10**.

5.5.5 Task 4: Configure DHCP Failover

1. On **SEA-ADM1**, in the **DHCP management console**, from the **IPv4** node, configure failover with **SEA-DC1** by using the following information for the failover relationship:
   - Relationship Name: **SEA-SVR1 to SEA-DC1**
   - Maximum Client Lead Time: **1 hour**
   - Mode: **Hot standby**
   - Role of Partner Server: **Standby**
   - Addresses reserved for standby server: **5%**
   - State Switchover Interval: **Disabled**
   - Enable Message Authentication: **Enabled**
   - Shared Secret: **DHCP-Failover**
2. Verify that **SEA-SVR1** only has one scope.
3. Verify that **SEA-DC1** has two scopes.

4. Under **SEA-DC1**, for the **Contoso** scope, configure failover with **172.16.10.12**, and reuse the existing failover relationship.
5. Verify that both scopes now appear on **SEA-SVR1**.

5.5.6 Task 5: Verify DHCP functionality

1. On **SEA-CL1**, configure the network connection to obtain an IP address and DNS server addresses automatically.
2. Examine the configuration status of the network connection to verify that the DHCP lease was obtained from **SEA-SVR2 (172.16.10.12)**.
3. Disable the Ethernet network connection.
4. On **SEA-ADM1**, in the **DHCP management console**, verify that both DHCP servers list the lease for **SEA-CL1** in the **Contoso** scope.
5. Stop the **DHCP** service on **SEA-SVR2 (172.16.10.12)**.
6. On **SEA-CL1**, enable the Ethernet network connection, and then verify that the same DHCP lease is obtained from **SEA-DC1 (172.16.10.10)**.

5.6 Exercise 2: Deploying and configuring DNS

5.6.1 Scenario

The staff who work at the Trey Research location within Contoso need to have their own DNS server to create records in their test environment. However, their test environment still needs to be able to resolve internet DNS names and resource records for Contoso. To meet these needs, you are configuring forwarding to your internet service provider (ISP) and creating a conditional forwarder for `contoso.com` to **SEA-DC1**. There is also a test application that needs a different IP address resolution based on user location. You are using DNS policies to configure `testapp.treyresearch.net` to resolve differently for users at the head office.

The main tasks for this exercise are as follows:

1. Install the DNS role.
2. Create a DNS zone.
3. Configure forwarding.
4. Configure conditional forwarding.
5. Configure DNS policies.
6. Verify DNS policy functionality.

5.6.2 Task 1: Install the DNS role

1. On **SEA-ADM1**, open **Microsoft Edge** and sign in to **Windows Admin Center**.
2. In **Windows Admin Center**, connect to **SEA-SVR1**.
3. From **Roles & features**, install the DNS role.
4. From **DNS**, install the **DNS PowerShell** tools. If **DNS** is not available in the **Tools pane** for **SEA-SVR1**, close **Microsoft Edge** and sign in to **Windows Admin Center** again.

5.6.3 Task 2: Create a DNS zone

1. On **SEA-ADM1**, in Windows Admin Center, create a new DNS zone with the following settings:
   - Zone type: **Primary**
   - Zone name: **`TreyResearch.net`**
   - Zone file: **Create a new file**
   - Zone file name: **`TreyResearch.net.dns`**
   - Dynamic update: **Do not allow dynamic update**
2. Create a new DNS record in the **`TreyResearch.net`** zone with the following settings:
   - DNS record type: **Host (A)**
   - Record name: **TestApp**
   - IP address: **172.30.99.234**
   - Time to live: **600**
3. At a Windows PowerShell prompt, run the following command to verify that the new record resolves properly:

```
Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net
```

5.6.4 Task 3: Configure forwarding

1. On **SEA-ADM1**, use **Server Manager** to open the **DNS Manager console**.
2. In **DNS Manager**, connect to **SEA-SVR1**.
3. In the properties of **SEA-SVR1**, on the **Forwarders** tab, configure **131.107.0.100** as a forwarder.

5.6.5 Task 4: Configure conditional forwarding

1. On **SEA-ADM1**, in **DNS Manager** for **SEA-SVR1**, create a new conditional forwarder for `Contoso.com` that directs requests to **172.16.10.10**.
2. Open a Windows PowerShell prompt and run the following command to verify that the conditional forwarder is working:

   ```
   Resolve-DnsName -Server sea-svr1.contoso.com -Name sea-dc1.contoso.com
   ```

5.6.6 Task 5: Configure DNS policies

1. On **SEA-ADM1**, in **Windows Admin Center**, while connected to **SEA-SVR1**, use **PowerShell** to sign in remotely.
2. At the **Windows PowerShell** prompt, run the following command to create a head office subnet:

   ```
   Add-DnsServerClientSubnet -Name "HeadOfficeSubnet" -IPv4Subnet "172.16.10.0/24"
   ```

3. Run the following command to create a zone scope for head office:

   ```
   Add-DnsServerZoneScope -ZoneName "TreyResearch.net" -Name "HeadOfficeScope"
   ```

4. Run the following command to create a new resource record for the head office scope:

   ```
   Add-DnsServerResourceRecord -ZoneName "TreyResearch.net" -A -Name "testapp" -IPv4Address "172.30.9
   ```

5. Run the following command to create a new policy that links the head office subnet and the zone scope:

   ```
   Add-DnsServerQueryResolutionPolicy -Name "HeadOfficePolicy" -Action ALLOW -ClientSubnet "eq,HeadOf
   ```

5.6.7 Task 6: Verify DNS policy functionality

1. On **SEA-CL1**, open a Windows PowerShell prompt, enter **ipconfig**, and then select Enter to verify that **SEA-CL1** is on the **HeadOffice subnet (172.16.10.0)**.
2. At the Windows PowerShell prompt, run the following command to test the DNS policy:

   ```
   Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net
   ```

3. Verify that **testapp** resolved to **172.30.99.100** as configured in **HeadOfficePolicy**.
4. Update **SEA-CL1** to use the following IPv4 configuration:
   - IP Address: **172.16.11.100**
   - Subnet mask: **255.255.0.0**
   - Default gateway: **172.16.10.1**
   - Preferred DNS server: **172.16.10.10**
5. At the Windows PowerShell prompt, run the following command to test the DNS policy:

   ```
   Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net
   ```

6. Verify that **testapp** resolved to **172.30.99.234**.

   Note: When the client is on the HeadOffice subnet (172.16.10.0/24), the record `testapp.treyresearch.net` resolves to 172.30.99.100. When the client is moved off of the HeadOffice subnet, `testapp.treyresearch.net` resolves to 172.30.99.234.

5.7 lab: title: 'Lab: Implementing storage solutions in Windows Server' module: 'Module 4: File servers and storage management in Windows Server'

6 Lab: Implementing storage solutions in Windows Server

6.1 Scenario

At Contoso, Ltd., you need to implement the Storage Spaces feature on the Windows Server 2019 servers to simplify storage access and provide redundancy at the storage level. Management wants you to test Data Deduplication to save storage. They also want you to implement Internet Small Computer System Interface (iSCSI) storage to provide a simpler solution for deploying storage in the organization. Additionally, the organization is exploring options for making storage highly available and researching the requirements that it must meet for high availability. You want to test the feasibility of using highly available storage, specifically Storage Spaces Direct.

6.2 Objectives

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

- Implement Data Deduplication.
- Configure Internet Small Computer System Interface iSCSI storage.
- Configure Storage Spaces.
- Implement Storage Spaces Direct.

6.3 Estimated time: 90 minutes

6.4 Lab setup

Virtual machines:

- For Exercises 1-3: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR3**, and **WS-011T00A-SEA-ADM1**
- For Exercise 4: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR1**, **WS-011T00A-SEA-SVR2**, **WS-011T00A-SEA-SVR3**, and **WS-011T00A-SEA-ADM1**

Username: Contoso\Administrator **Password:** Pa55w.rd

> **Note:** You must revert the virtual machines (VM) between each exercise. Because most of the VMs are Windows Server 2019 Server Core VMs, the time to revert and restart is faster than trying to undo changes made to the storage environment in the exercises.

6.5 Lab exercise 1: Implementing Data Deduplication

6.5.1 Scenario

You decide to install the Data Deduplication role service by using Server Manager. You determine that drive **M** is heavily used, and you suspect that it contains duplicate files in some folders. You decide to enable and configure the Data Deduplication role to reduce the consumed space on this volume.

The main tasks for this exercise are:

1. Install the Data Deduplication feature on **SEA-SVR3**.
2. Enable and configure Data Deduplication on drive **M** on **SEA-SVR3**.
3. Test Data Deduplication by adding files and observing deduplication.

6.5.2 Task 1: Install the Data Deduplication role service

1. On **SEA-ADM1**, in Server Manager, add the **Data Deduplication** role to **SEA-SVR3** (under File and Storage Services, and then under File and iSCSI Services).

2. Share the (**SEA-ADM1**) **C:\Labfiles** folder adding the **Users** group with **Read** access.

3. On **SEA-SVR3**, in Windows PowerShell, create a virtual disk on **SEA-SVR3** from disk 1, and label it drive **M**. Use the following commands to complete this:

   ```
   Get-Disk
   ```

```
Initialize-Disk -Number 1

New-Partition -DiskNumber 1 -UseMaximumSize -DriveLetter M

Format-Volume -DriveLetter M -FileSystem ReFS
```

4. Exit Windows PowerShell and map drive **X** to **\\SEA-ADM1\Labfiles** (NET USE), and then in the drive **X:**, browse to **cd Mod04**, and then get a directory listing.
5. In the **Windows PowerShell command** window, enter **M:**
6. Enter **MD Data**
7. Copy **x:\mod04\createlabfiles.cmd M:**.
8. Enter the **CreateLabFiles.cmd**.
9. Enter **cd data**, then enter **dir**.
10. Notice that **M:\Data** has free space. Make note of the amount in bytes.

6.5.3 Task 2: Enable and configure Data Deduplication

1. Return to **SEA-ADM1**.
2. In Server Manager, select **File and Storage Services**, and then on **SEA-SVR3**, select **Disks**.
3. Select the **1** disk, and then select the **M** volume.
4. Enable Data Deduplication, and then select the **General purpose file server** setting.
5. Configure the following settings:
   - Deduplicate files older than (in days): **0**
   - Enable throughput optimization: Selected

6.5.4 Task 3: Test Data Deduplication

1. On **SEA-ADM1**, open **WAC**.
2. Connect to **SEA-SVR3**, and then open the **PowerShell** node.
3. Execute the following command to start Data Deduplication process, and then select Enter:

   ```
   Start-DedupJob m: -Type Optimization -Memory 50
   ```

4. Switch to **SEA-SVR3**. In the Command Prompt window, enter **Dir**. Observe the Bytes free size on property values for the Data Directory.
5. Wait for 5 to 10 minutes to allow the deduplication job to run.
6. Switch back to the Windows PowerShell window on **SEA-ADM1**.
7. To verify the Data Deduplication status, run the following commands, selecting Enter at the end of each line:

   ```
   Get-DedupStatus -Volume M: | fl

   Get-DedupVolume -Volume M: |fl

   Get-DedupMetadata -Volume M: |fl
   ```

8. In Server Manager, select **File and Storage Services**, select Disk **1**, and then select Volume **M** (You might have to refresh).
9. Observe the values for **Deduplication Rate** and **Deduplication Savings**.
10. Close all open windows except **Server Manager**.

    When you have finished the exercise, revert the VMs to their initial state.

6.6 Lab exercise 2: Configuring iSCSI storage

6.6.1 Scenario

Executives at Contoso are exploring the option of using iSCSI to decrease the cost and complexity of configuring centralized storage. To test this, you must install and configure the iSCSI targets, and configure the iSCSI initiators to provide access to the targets.

The main tasks for this exercise are:

1. Install iSCSI and configure targets on **SEA-SVR3**.
2. Connect to and configure iSCSI targets from **SEA-DC1** (initiator).
3. Verify iSCSI disk presence by copying and moving files.

6.6.2 Task 1: Install iSCSI and configure targets

1. On **SEA-ADM1**, open a Windows PowerShell window.
2. Enter the following command, and then select Enter:

   ```
   Invoke-Command -ComputerName SEA-SVR3 -ScriptBlock {Install-WindowsFeature -Name FS-iSCSITarget-Se
   ```

3. On **SEA-ADM1**, open a remote Windows PowerShell session to **SEA-SVR3** as **Contoso\Administrator**.
4. Use Windows PowerShell to initialize, create, and format a volume as Resilient File System (ReFS) on the two offline disks (disks 2 and 3) on **SEA-SVR3** (where X refers to the drive number). Use the following three commands, selecting Enter after each line:

   ```
   Initialize-Disk -Number <X>
   New-Partition -DiskNumber <X> -UseMaximumSize -AssignDriveLetter
   ```

   Note the drive letter it assigns because you'll be using it in the next command.

   ```
   Format-Volume -DriveLetter <X> -FileSystem ReFS
   ```

5. Use Windows PowerShell to create an inbound and outbound Firewall exception for port 3260. Use the following commands, selecting Enter at the end of each line:

   ```
   New-NetFirewallRule -DisplayName "iSCSITargetIn" -Profile "Any" -Direction Inbound -Action Allow -
   ```

   ```
   New-NetFirewallRule -DisplayName "iSCSITargetOut" -Profile "Any" -Direction Outbound -Action Allow
   ```

   Note: Word wrap is used to display the previous command. Don't use word wrap when entering the command in Windows PowerShell.

6. Close the remote session but keep Windows PowerShell open.

6.6.3 Task 2: Connect to and configure iSCSI targets

1. On **SEA-ADM1**, in the **Server Manager** window, in **File and Storage Services**, under **Disks**, select the **SEA-DC1** server. Note that it only contains the boot and system volume drive C.
2. In Server Manager, in **File and Storage Services**, under **iSCSI**, select the **SEA-SVR3** server.
3. Create a new iSCSI virtual disk with the following settings:
   - Storage Location: **E:**
   - Name: **iSCSIDisk1**
   - Disk size: **5 GB**, **Dynamically Expanding**
   - iSCSI target: **New**
   - Target name: **iSCSIFarm**
   - Access servers: **SEA-DC1** (Browse and check names)
4. Create a second iSCSI virtual disk with the following settings:
   - Storage Location: **F:**
   - Name: **iSCSIDisk2**
   - Disk size: **5 GB**, **Dynamically Expanding**
   - iSCSI target: **iSCSIFarm**

5. On **SEA-DC1**, open Windows PowerShell, enter the following commands, selecting Enter at the end of each line:

   ```
   Start-Service msiscsi

   iscsicpl
   ```

   Note: The **iscsicpl** command will open an **iSCSI Initiator Properties** dialog box.

6. Connect to the following iSCSI target:

   - Name: **SEA-SVR3**
   - Target name: **iqn.1991-05.com.microsoft:SEA-SVR3-fileserver-target**

6.6.4 Task 3: Verify iSCSI disk presence

1. In Server Manager, on **SEA-ADM1**, in the **tree** pane, select **File and Storage Services**, and then select **Disks**.
2. Notice the two new 5-gigabyte (GB) disks on the **SEA-DC1** server that are offline. Notice that the bus entry is **iSCSI**. (If you're in the **File and Storage Services** section of **Server Manager**, you might need to select the refresh button to open the two new disks.)

   Note: When you have finished the exercise, revert the VMs to their initial state.

6.7 Lab exercise 3: Configuring redundant Storage Spaces

6.7.1 Scenario

To meet some requirements for high availability, you decided to evaluate redundancy options in Storage Spaces. Additionally, you want to test the provisioning of new disks to the storage pool.

The main tasks for this exercise are:

1. Create a storage pool by using the iSCSI disks attached to **SEA-SVR3**.
2. Create a three-way mirrored disk on **SEA-SVR3**.
3. Copy a file to the volume on the three-way mirror, and verify it's present in File Explorer.
4. Disconnect the disk and verify file availability.
5. Add a new disk to storage pool.

   Note: In **Windows Server 2019**, you can't disconnect a disk in a storage pool. You can only remove it. You also can't remove a disk from a three-way mirror without adding a new disk first.

6.7.2 Task 1: Create a storage pool by using the iSCSI disks attached to the server

1. On **SEA-ADM1**, open Server Manager.
2. In Server Manager, in **File and Storage Services**, select **Disks**.
3. Set the disks 1-4 for **SEA-SVR3** to **Online**.
4. In Server Manager, on **SEA-SVR3**, create a new storage pool named **SP1**.
5. Use three of the four available disks to make up the pool.

6.7.3 Task 2: Create a three-way mirrored disk

1. In Server Manager, in **Storage Pools**, in **SP1**, create a new virtual disk named **Three-Mirror** that uses a mirror storage layout, and thin provisioning. Use **25 GB** for the size.
2. Create a new volume from **Three-Mirror** named **TestData**.
3. Format it as ReFS, and assign it drive letter **T**.
4. Close Server Manager.

6.7.4 Task 3: Copy a file to the volume, and verify it's present in File Explorer

1. Switch to **SEA-SVR3**.
2. In Windows PowerShell, enter the following command, and then select Enter:

   ```
   netsh advfirewall firewall set rule group=&quot;File and Printer Sharing&quot; new enable=Yes
   ```

3. Switch back to **SEA-ADM1**. In the **File Explorer** window, in the Address bar, enter **\\sea-svr3\t$.**

4. Create a new folder named **Test Data**, and then create a new document named **Document1.txt** in that folder.

6.7.5 Task 4: Disconnect the disk and verify file availability

1. In Server Manager, on **SEA-ADM1**, add a new physical disk to storage pool **SP1**. Ensure the disk uses automatic allocation.
2. Remove the top disk in the **PHYSICAL DISKS** pane from the storage pool.
3. Return to **Document1.txt**, add some text, and then save it.

6.7.6 Task 5: Add a new disk to the storage pool

1. In Server Manager, re-scan the **SP1** storage pool.
2. Add the disk you removed earlier, ensuring it's allocated automatically.
3. Open **Document1.txt**, add some more text, and then save it.
4. Switch back to **SEA-SVR3**.
5. On drive **T**, in the new **Test Data** folder, open **Document1.txt**.
6. Close all open windows.

When you have finished the exercise, revert the VMs to their initial state.

6.8 Lab exercise 4: Implementing Storage Spaces Direct

6.8.1 Scenario

You want to test whether using local storage as highly available storage is a viable solution for your organization. Previously, your organization has only used storage area networks (SANs) for storing VMs. The new features in Windows Server 2019 make it possible to use only local storage, so you want to implement Storage Spaces Direct as a test implementation.

The main tasks for this exercise are:

1. Install the Storage Spaces Direct Failover Clustering features.
2. Create and validate the failover cluster.
3. Enable Storage Spaces Direct.
4. Create the storage pool, a virtual disk, and a share.
5. Verify that Storage Spaces Direct functions properly.

6.8.2 Task 1: Install the Storage Spaces Direct Failover Clustering features

1. On **SEA-ADM1**, open Server Manager.
2. Ensure all servers refer to **Manageability** of **Online-Performance counters not started**.
3. In **Server Manager**, in the navigation pane, select **File and Storage Services**, and then select **Disks**.
4. In the **Disks** pane, scroll until you find **SEA-SVR3*, disks 1 through 4, and note that they are set to **Unknown**.
5. Right-click or access the context menu for each offline disk, select **Bring Online**, and then in the **Bring Disk Online** window, select **Yes**.
6. Verify that all disks are online for **SEA-SVR1** and **SEA-SVR2**.
7. Open Windows PowerShell ISE and load the **C:\Labfiles\Mod04\Implement-StorageSpacesDirect.ps1** script.

   > **Note:** This script is divided into numbered steps. There are eight steps, and each step has a number of commands. Run the commands by highlighting each and selecting **F8**, one after the other in accordance with the following instructions. Ensure each step finishes, that is, goes from Stop operation (a red square) to Run selection (a green arrow) in the menu bar, before starting the next step.

8. Run the commands in Step 1. This command installs the Failover Clustering role service on **SEA-SVR1**, **SEA-SVR2** and **SEA-SVR3**. The second command restarts the three servers, which is required to complete the install, and the third command installs the Failover Cluster Manager console on **SEA-ADM1**.

Note: When you start the second command to restart the servers, you can run the third command to install the console without waiting for the second command's restarts to finish.

6.8.3 Task 2: Create and validate a cluster

1. On **SEA-ADM1**, start the **Failover Cluster Manager** tool.
2. In **Windows PowerShell ISE**, run the step 2 command, which will take approximately 5 minutes to finish.
3. Ensure the output only includes nothing greater than warnings.
4. In **Windows PowerShell ISE**, run the step 3 command.
5. When the command completes, return to **Failover Cluster Manager**, and add the cluster named `S2DCluster.Contoso.com`.

6.8.4 Task 3: Enable Storage Spaces Direct

1. In **Windows PowerShell ISE**, run the step 4 command, which will take approximately 5 minutes to finish.
2. Run the step 5 command, which creates the **S2DStoragePool** storage pool.
3. Return to the **Failover Cluster Manager**, and then observe the **Cluster Pool 1** object in **Pools**.
4. Return to **Windows PowerShell ISE**, and run the step 6 command, which creates the **CSV** file system.
5. Return to the **Failover Cluster Manager**, and then observe the **Cluster Virtual Disk (CSV)** object in **Disks**.

6.8.5 Task 4: Create a storage pool, a virtual disk, and a share

1. In **Windows PowerShell ISE**, run the step 7 command, which creates the **S2D-SOFS** service role.
2. Return to the **Failover Cluster Manager**, and then observe the **S2D-SOFS** object in **Roles**.
3. Return to **Windows PowerShell ISE**, and run all three commands in Step 8 simultaneously to create the **VM01** share. To run them simultaneously, highlight all three and then select **F8**.
4. Return to the **Failover Cluster Manager**, and then observe the **VM01** object in **Shares**.

6.8.6 Task 5: Verify Storage Spaces Direct functionality

1. On **SEA-ADM1**, in File Explorer, open **\s2d-sofs\VM01** and create a folder named **VMFolder**.
2. In **Windows PowerShell ISE**, enter the following command, and then select Enter:

   ```
   Stop-Computer -ComputerName SEA-SVR3
   ```

3. Return to Server Manager and confirm **SEA-SVR3** is included in the list of **All Servers**.
4. Return to the **Failover Cluster Manager**, and then observe the **Cluster Virtual Disk (CSV)** information in the **Disks** node. (Notice the **Health Status** is set to **Warning**, and the **Operational Status** is **Degraded**.)
5. On **SEA-ADM1**, open the **Windows Admin Console (WAC)**.
6. If required, sign in as **Contoso\Administrator** with a password of **Pa55w.rd**.
7. On the **All connections** page, select **+ Add**.
8. Scroll to find and select **Windows Server Cluster**, and then enter `S2DCluster.Contoso.com` as the cluster name.
9. Notice that the pass-through credentials will be denied; however, you can manually add the same account for the connection. Reenter the sign-in information **Contoso\Administrator** with a password of **Pa55w.rd** in the other credentials area.
10. Notice that the scroll to select completion feature won't work, so simply select Enter.
11. Don't add the other servers in the cluster as they are already registered in **WAC**.
12. Note the cluster has a critical error because **SEA-SVR3** is offline. Start **SEA-SVR3**.
13. After a few minutes, verify that the alert clears.
14. Close all windows and revert the VMs.

6.8.7 Results

After completing this lab, you will have:

- Tested the implementation of Data Deduplication.
- Installed and configured iSCSI storage.
- Configured redundant Storage Spaces.
- Tested the implementation of Storage Spaces Direct.

6.9 lab: title: 'Lab: Implementing and configuring virtualization in Windows Server' module: 'Module 5: Hyper-V virtualization and containers in Windows Server'

7 Lab: Implementing and configuring virtualization in Windows Server

7.1 Scenario

Contoso is a global engineering and manufacturing company with its head office in Seattle, USA. An IT office and data center are in Seattle to support the Seattle location and other locations. Contoso recently deployed a Windows Server 2019 server and client infrastructure.

Because of many physical servers being currently underutilized, the company plans to expand virtualization to optimize the environment. Because of this, you decide to perform a proof of concept to validate how Hyper-V can be used to manage a virtual machine environment. Also, the Contoso DevOps team wants to explore container technology to determine whether they can help reduce deployment times for new applications and to simplify moving applications to the cloud. You plan to work with the team to evaluate Windows Server containers and to consider providing Internet Information Services (Web services) in a container.

7.2 Objectives

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

- Create and configure VMs.
- Install and configure containers.

7.3 Lab Setup

Estimated Time: 60 minutes

Virtual Machines: WS-011T00A-SEA-DC1, WS-011T00A-SEA-ADM1, and WS-011T00A-SEA-SVR1

User Name: Contoso\Administrator

Password: Pa55w.rd Note that Internet access is required to successfully complete the second exercise in this lab.

7.4 Lab Startup

1. Select **SEA-DC1**.
2. Sign in by using the following credentials:
   - User name: **Administrator**
   - Password: **Pa55w.rd**
   - Domain: **Contoso**
3. Repeat these steps for **SEA-ADM1** and **SEA-SVR1**.

7.5 Exercise 1: Creating and configuring VMs

7.5.1 Exercise scenario

In this exercise, you will use Hyper-V Manager and Windows Admin Center to create and configure a virtual machine. You will start with creating a private virtual network switch. Next you decide to create a differencing

drive of a base image that has already been prepared with the operating system to be installed on the VM. Finally, you will create a generation 1 VM that uses the differencing drive and private switch that you have prepared for the proof of concept.

The main tasks for this exercise are:

1. Create a Hyper-V virtual switch
2. Create a virtual hard disk
3. Create a virtual machine
4. Manage virtual machines using Windows Admin Center

7.5.2 Task 1: Create a Hyper-V virtual switch

1. On SEA-ADM1, open **Server Manager**.
2. In Server Manager, select **All Servers**.
3. In the Servers list, select and hold (or right-click) or access the context menu **SEA-SVR1** and then select **Hyper-V Manager**.
4. Use the **Virtual Switch Manager** to create the following switch:
   - Name: **Contoso Private Switch**
   - Connection type: **Private network**

7.5.3 Task 2: Create a virtual hard disk

1. On SEA-ADM1, in Hyper-V Manager, use the **New Virtual Hard Disk Wizard** to create a new virtual hard disk as follows:
   - Disk Format: **VHD**
   - Disk Type: **Differencing**
   - Name: **SEA-VM1**
   - Location: **C:\Base**
   - Parent Disk: **C:\Base\BaseImage.vhd**

7.5.4 Task 3: Create a virtual machine

1. On SEA-ADM1, in Hyper-V Manager, create a new virtual machine as follows:
   - Name: **SEA-VM1**
   - Location: **C:\Base**
   - Generation: **Generation 1**
   - Memory: **4096**
   - Networking: **Contoso Private Switch**
   - Hard disk: **C:\Base\SEA-VM1.vhd**
2. Open the **Settings** for **SEA-VM1** and enable **Dynamic Memory** with a Maximum RAM value of **4096**.
3. Close Hyper-V Manager.

7.5.5 Task 4: Manage Virtual Machines using Windows Admin Center

1. On SEA-ADM1, on the taskbar, select **Microsoft Edge**.
2. In Microsoft Edge, on the Favorites Bar, select **Windows Admin Center**.
3. In the Windows Security box, enter **Contoso\Administrator** with the password of **Pa55w.rd** and then select **OK**.
4. In the **All connections** list, select **SEA-SVR1**.

   Note: You may need to select **Manage As** to then enter the credentials in the next step.
5. In the **Specify your credentials** page, select **Use another account for this connection**, and then enter **Contoso\Administrator** with the password of **Pa55w.rd**.
6. In the **Tools** list, select **Virtual Machines**. Review the Summary pane.
7. On SEA-VM1, create a new disk, 5 GB in size.

Note: The **Save Disk** Setting may be greyed out which is a known issue. A workaround would be to create the disk in Hyper-V if needed.

8. Start **SEA-VM1** and then display the statistics for the running VM.
9. Refresh the page and then shut down the VM.
10. In the **Tools** list, select **Virtual switches** and identify the existing switches.
11. Close all open windows on SEA-ADM1.

7.5.6 Exercise 1 results

After this exercise, you should have used Hyper-V Manager and Windows Admin Center to create a virtual switch, create a virtual hard disk, and then create and manage a virtual machine.

7.6 Exercise 2: Installing and configuring containers

7.6.1 Exercise Scenario

In this exercise, you will use Docker to install and run Windows containers. You will also use Windows Admin Center to manage containers.

The main tasks for this exercise are:

1. Install Docker on Windows Server
2. Install and run a Windows container
3. Use Windows Admin Center to manage containers

7.6.2 Task 1: Install Docker on Windows Server

1. On SEA-ADM1, open **Windows Admin Center** using the Contoso\Administrator credentials.
2. Connect to **SEA-SVR1** using the Contoso\Administrator credentials and then connect to the server using PowerShell.

   Note: The Powershell connection in **WAC** may be slow due to nested virtualization used in the lab, so an alternate method is to use **Enter-PSSession -computername SEA-SVR1** from a Powershell window on **SEA-ADM1**.

3. At the PowerShell command prompt enter the following command and then select Enter:

   ```
   Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
   ```

4. At the PowerShell command prompt enter the following command and then select Enter:

   ```
   Install-Package -Name docker -ProviderName DockerMsftProvider
   ```

5. After the installation is complete, restart the computer by using the following command:

   ```
   Restart-Computer -Force
   ```

7.6.3 Task 2: Install and run a Windows container

1. After SEA-SVR1 restarts reconnect the PowerShell tool and provide the Contoso\Administrator credentials.
2. Verify the installed version of Docker by using the following command:

   ```
   Get-Package -Name Docker -ProviderName DockerMsftProvider
   ```

   Note: You may need to run **Start-Service -name Docker** before running the next commands.

3. To verify whether any Docker images are currently pulled, use the following command:

   ```
   Docker images
   ```

4. To review docker base images from the online Microsoft repository, use the following command:

   ```
   Docker search Microsoft
   ```

   Note: You may disregard any errors and continue with the next step.

5. To download a server core image, with IIS, that matches the host operating system, run the following command:

   ```
   docker pull mcr.microsoft.com/windows/servercore/iis:windowsservercore-ltsc2019
   ```

   Note: This download may take more than 15 minutes to complete.

6. To verify the Docker image that is currently pulled, use the following command:

   ```
   Docker images
   ```

7. To run the container, enter the following command:

   ```
   Docker run -d -p 80:80 --name ContosoSite mcr.microsoft.com/windows/servercore/iis:windowsserverco
   cmd
   ```

   This command runs the IIS image as a background service (-d) and configures networking such that port 80 of the container host maps to port 80 of the container.

8. Enter the following command to retrieve the IP address information of the container host:

   ```
   ipconfig
   ```

   Note the IPv4 address of the Ethernet adapter named vEthernet (nat). This is the address of the new container. Make a note of the IPv4 address of the Ethernet adapter named **Ethernet**. This is the IP address of the Host (SEA-SVR1).

9. In Microsoft Edge, open another tab and then enter `<http://172.16.10.12>`. Observe the default IIS page.

10. In the remote PowerShell session, enter the following command:

    ```
    docker ps
    ```

    This command provides information on the container that is currently running on SEA-SVR1. Take note of the container ID as you will use it to stop the Container.

11. In the remote PowerShell session, enter the following command:

    ```
    docker stop *<ContainerID>*
    ```

12. Rerun the `docker ps` command to confirm that the container has stopped.

7.6.4 Task 3: Use Windows Admin Center to manage containers

1. On SEA-ADM1, ensure that SEA-SVR1 is targeted in the Windows Admin Center and then select the **Containers** tool.
2. Browse through each of the **Summary**, **Containers**, **Images**, **Networks**, and **Volumes** tabs.

7.6.5 Exercise 2 results

7.7 After this exercise, you should have installed Docker on Windows Server and installed and run a Windows container containing web services.

7.8 lab: title: 'Lab: Implementing failover clustering' module: 'Module 6: High availability in Windows Server'

8 Lab: Implementing failover clustering

8.1 Scenario

As the business of Contoso, Ltd. grows, it's becoming increasingly important that many of the applications and services on its network are always available. Contoso has many services and applications that must be available to internal and external users who work in different time zones around the world. Many of these applications can't be made highly available by using Network Load Balancing (NLB). Therefore, you should use a different technology to make these applications highly available.

As one of the senior network administrators at Contoso, you're responsible for implementing failover clustering on the servers that are running Windows Server 2019 to provide high availability for network services and applications. You're also responsible for planning the failover cluster configuration and deploying applications and services on the failover cluster.

8.2 Objectives

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

- Configure a failover cluster.
- Deploy and configure a highly available file server on the failover cluster.
- Validate the deployment of the highly available file server.

8.3 Estimated time: 60 minutes

8.4 Lab setup

Virtual machines: **SEA-DC1**, **SEA-ADM1**, **SEA-SVR2**, and **SEA-SVR3**

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

Sign in only to **SEA-ADM1**. Sign in to other virtual machines only when instructed in lab steps.

8.5 Exercise 1: Configuring iSCSI storage

8.5.1 Scenario

Contoso has important applications and services that it wants to make highly available. Some of these services can't use NLB, so you have decided to implement failover clustering. You decide to use Internet SCSI (iSCSI) storage for failover clustering. First, you'll configure iSCSI storage to support your failover cluster.

The main tasks for this exercise are to:

- Install Failover Clustering.
- Configure iSCSI virtual disks.

8.5.2 Task 1: Install Failover Clustering

1. On **SEA-ADM1**, use Windows PowerShell to install the **Failover-Clustering** feature with Management Tools and the **FS-iSCSITarget-Server** feature.
2. Create remote PowerShell sessions for **SEA-SVR2** and **SEA-SVR3** to install the **Failover-Clustering** feature with Management Tools.
3. After Failover Clustering is installed on **SEA-ADM1**, **SEA-SVR2**, and **SEA-SVR3**, restart all three computers.

8.5.3 Task 2: Configure iSCSI virtual disks

1. Create three iSCSI virtual disks on **SEA-ADM1** by using the **New-IscsiVirtualDisk** cmdlet with the following values:
   - Disk1:
     - Storage location: **C:\storage**
     - Disk name: **Disk1**
     - Size: **10 GB**
   - Disk2:
     - Storage location: **C:\storage**
     - Disk name: **Disk2**
     - Size: **10 GB**
   - Disk3:
     - Storage location: **C:\storage**
     - Disk name: **Disk3**
     - Size: **10 GB**
2. Use the **Start-Service** and **Set-Service** cmdlets to start the **msiscsi** service on **SEA-SVR2** and **SEA-SVR3**, configuring the service to start automatically.
3. Create a new iSCSI target on **SEA-ADM1** by using the **New-IscsiServerTarget** cmdlet with the following values:
   - Target name: **ISCSI-MOD6**
   - InitiatorsIds:

- **"IQN:iqn.1991-05.com.microsoft:sea-svr2.contoso.com"**
- **"IQN:iqn.1991-05.com.microsoft:sea-svr3.contoso.com"**

8.5.4 Results

After completing this exercise, you should have successfully installed the Failover Clustering feature and configured the iSCSI Target Server.

8.6 Exercise 2: Configuring a failover cluster

8.6.1 Scenario

In this exercise, you'll configure a failover cluster. You'll implement the core components for failover clustering. You'll validate the cluster and then create the failover cluster.

The main tasks for this exercise are to:

1. Connect clients to the iSCSI targets.
2. Initialize the disks.
3. Validate and create a failover cluster.

8.6.2 Task 1: Connect clients to the iSCSI targets

1. On **SEA-ADM1**, use PowerShell with the **Add-IscsiVirtualDiskTargetMapping** cmdlet to map the disks that you created in the previous exercise to the **ISCSI-MOD6** target.
2. Use a remote PowerShell session to **SEA-SVR2** to connect to the **iSCSI Target Portal** by running the following commands:

```
New-iSCSITargetPortal -TargetPortalAddress SEA-ADM1.contoso.com

Connect-iSCSITarget - NodeAddress iqn.1991-05.com.microsoft:sea-adm1.contoso.com

Get-iSCSITarget | fl
```

3. Verify that after you run the **Get-iSCSITarget** command, the value for the *IsConnected* variable is True.
4. Repeat steps 2 and 3 for **SEA-SVR3**.

8.6.3 Task 2: Initialize the disks

1. On **SEA-SVR2**, use Windows PowerShell and the **Initialize-Disk**, **New-Partition**, and **Format-Volume** cmdlets to configure the three disks with the following settings:
   - PartitionStyle: **MBR**
   - New-Partition Size: **5GB**
   - File System : **NTFS**
   - Assign drive letter automatically

8.6.4 Task 3: Validate and create a failover cluster

1. Sign in to **SEA-SVR2** locally as **Contoso\Administrator**.
2. Use the **Test-Cluster SEA-SVR2, SEA-SVR3** cmdlet to start the **Validate a Configuration Wizard**.
3. Review the results. No errors should appear, but some warnings are expected.
4. Use the **New-Cluster -Name WFC2019 -Node sea-svr2 -StaticAddress 172.16.10.125** command to create a new cluster.
5. Use the **Add-ClusterNode** cmdlet to add **SEA-SVR3** as a cluster node.

8.6.5 Results

After completing this exercise, you should have configured disks and created a failover cluster.

8.7 Exercise 3: Deploying and configuring a highly available file server

8.7.1 Scenario

At Contoso, file services are important services that must be made highly available. After you have created a cluster infrastructure, you decide to configure a highly available file server and then implement settings for failover and failback.

The main tasks for this exercise are to:

1. Add the file server application to the failover cluster.
2. Add a shared folder to a highly available file server.
3. Configure the failover and failback settings.

8.7.2 Task 1: Add the file server application to the failover cluster

1. On **SEA-ADM1**, open the **Failover Cluster Manager** console.
2. Connect to the **WFC2019** cluster.
3. In the **Nodes** node, check that both of the **SEA-SVR2** and **SEA-SVR3** nodes are running.
4. In the **Storage** node, select **Disks**, and then verify that three cluster disks are online.
5. Add **File Server** as a cluster role, and then select the **File Server for general use** option.
6. Specify the following settings:
   - Client Access Name: **FSCluster**
   - Address: **172.16.0.130**
   - Storage: **Cluster Disk 1, Cluster Disk 2**
7. Close the wizard.

8.7.3 Task 2: Add a shared folder to a highly available file server

1. On **SEA-ADM1**, in the **Failover Cluster Manager** console, select to add a file share to the **FSCluster** role.
2. Specify the file share profile as **SMB Share - Quick**.
3. Accept the default values on the **Select the server and the path for this share** page.
4. Name the shared folder **Docs**.
5. Accept the default values on the **Configure share settings** and **Specify permissions to control access** pages.
6. At the end of the **New Share** wizard, create the share.

8.7.4 Task 3: Configure the failover and failback settings

1. On **SEA-ADM1**, in the **Failover Cluster Manager** console, open the properties for the **FSCluster** cluster role.
2. Set failback for **between 4 and 5 hours**.
3. Select both **SEA-SVR2** and **SEA-SVR3** as the **Preferred owners**.
4. Move **SEA-SVR3** to be the first in the preferred owners list.

8.7.5 Results

After completing this exercise, you should have configured a highly available file server.

8.8 Exercise 4: Validating the deployment of the highly available file server

8.8.1 Scenario

In implementing a failover cluster, you want to perform failover and failback tests. Additionally, you want to change the witness disk in the quorum.

The main tasks for this exercise are to:

1. Validate the highly available file server deployment.
2. Validate the failover and quorum configuration for the File Server role.

8.8.2 Task 1: Validate the highly available file server deployment

1. On **SEA-ADM1**, open File Explorer, and then try to access the **\\FSCluster** location.
2. Verify that you can access the **Docs** folder.

3. Create a test text document inside this folder.
4. On **SEA-ADM1**, in the **Failover Cluster Manager** console, move **FSCluster** to another node.
5. On **SEA-ADM1**, in File Explorer, verify that you can still access the **FSCluster** location.

8.8.3 Task 2: Validate the failover and quorum configuration for the File Server role

1. On **SEA-ADM1**, in **Failover Cluster Manager**, determine the current owner for the **FSCluster** role.
2. Stop the Cluster service on the node that's the current owner of the **FSCluster** role.
3. Try to access **FSCluster** from File Explorer to verify that **FSCluster** has moved to another node and that the **FSCluster** location is still available.
4. Start the Cluster service on the node on which you stopped it in step 2.
5. Configure cluster quorum for **FSCluster** to use the default quorum configuration.
6. Browse to the **Disks** node, and then take the disk marked **witness disk in Quorum** offline.
7. Verify that **FSCluster** is still available by trying to access it from File Explorer on **SEA-ADM1**.
8. Bring the witness disk online.

8.8.4 Results

After completing this exercise, you should have validated high availability with Failover Clustering.

8.9 lab: title: 'Lab: Implementing Hyper-V Replica and Windows Server Backup' module: 'Module 7: Disaster Recovery in Windows Server'

9 Lab: Implementing Hyper-V Replica and Windows Server Backup

9.1 Scenario

You're working as an administrator at Contoso, Ltd. Contoso wants to assess and configure new disaster recovery and backup features and technologies. As the system administrator, you have been tasked with performing that assessment and implementation. You decided to evaluate **Hyper-V Replica** and Windows Server Backup.

9.2 Objectives

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

- Configure and implement **Hyper-V Replica**.
- Configure and implement backup with Windows Server Backup.

9.3 Lab setup

Estimated time: **45 minutes**

Virtual machines: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR1**, **WS-011T00A-SEA-SVR2**, and **WS-011T00A-SEA-ADM1**

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

1. Ensure that the **SEA-DC1**, **SEA-ADM1**, **SEA-SVR1**, and **SEA-SVR2** virtual machines (VMs) are running.
2. Select **SEA-ADM1**.
3. Sign in by using the following credentials:
   - User name: **Administrator**
   - Password: **Pa55w.rd**
   - Domain: **Contoso**
4. When instructed in the lab, repeat these steps for **SEA-DC1**, **SEA-SVR1**, and **SEA-SVR2**.

9.4 Exercise 1: Implementing Hyper-V Replica

9.4.1 Scenario

Before you start with a cluster deployment, you have decided to evaluate the new technology in Hyper-V for replicating VMs between hosts. You want to be able to manually mount a copy of a VM on another host if the active copy or host fails.

The main tasks for this exercise are to:

1. Configure a replica on both host machines: **SEA-SVR1** and **SEA-SVR2**.
2. Configure replication for the **SEA-CORE1** VM.
3. Validate a failover.

9.4.2 Task 1: Configure a replica on both host machines

1. On **SEA-ADM1**, open Windows PowerShell as an administrator.
2. In the PowerShell window, create a new remote PowerShell session to **sea-svr1.contoso.com**. Use **Contoso\Administrator** credentials to connect to the remote PowerShell on **SEA-SVR1**.
3. In the remote PowerShell session on **sea-svr1.contoso.com**, use the **Enable-Netfirewallrule** cmdlet to enable the firewall rule named Hyper-V Replica HTTP Listener (TCP-In).
4. Use the **Get-Netfirewallrule** cmdlet to verify that the Hyper-V Replica HTTP Listener (TCP-In) rule is enabled.
5. Use the following command to configure **SEA-SVR1** for **Hyper-V Replica**:

   ```
   Set-VMReplicationServer -ReplicationEnabled $true -AllowedAuthenticationType Kerberos -ReplicationA
   ```

6. Use the **Get-VM** cmdlet to verify that the **SEA-CORE1** VM is present on **SEA-SVR1**.
7. Open a new remote PowerShell session for **sea-svr2.contoso.com** in a new PowerShell window. Repeat steps 2 through 5 to configure **SEA-SVR2** for **Hyper-V Replica**.

9.4.3 Task 2: Configure replication

1. Switch to the PowerShell window where you have the remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following command, and then select Enter:

   ```
   Enable-VMReplication SEA-CORE1 -ReplicaServerName SEA-SVR2.contoso.com -ReplicaServerPort 80 -Auth
   ```

2. Start replication with the following command:

   ```
   Start-VMInitialReplication SEA-CORE1
   ```

3. After you've verified that you didn't receive any error message from the previous command, enter the following command, and then select Enter:

   ```
   Get-VMReplication
   ```

   This command retrieves the replication status.

   In the result table, search for the value in the **State** column. It should be **InitialReplicationInProgress**. Wait for 4–5 minutes, and then repeat this command. Verify that the value in the **State** column is **Replicating**. Don't proceed to the next steps until you get this value. Also ensure that **Primary server** is set to **SEA-SVR1** and that **ReplicaServer** is set to **SEA-SVR2**.

4. Switch to the PowerShell window where you have the remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   get-vm
   ```

   Verify that you now have the **SEA-CORE1** VM on **SEA-SVR2**. This means that the VM successfully replicated.

9.4.4 Task 3: Validate failover

1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following command, and then select Enter:

```
Start-VMFailover -Prepare -VMName SEA-CORE1 -computername SEA-SVR1.contoso.com
```

2. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Start-VMFailover -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com
   ```

3. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Set-VMReplication -Reverse -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com
   ```

4. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Start-VM -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com
   ```

5. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Get-VM
   ```

   In the result table, search for the value in the **State** column. It should be **Running**.

6. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Get-VMReplication
   ```

   In the result table, search for the value the in the **State** column. It should be **Replicating**. Additionally, ensure that the **Primary server** is now set to **SEA-SVR2** and that **ReplicaServer** is set to **SEA-SVR1**.

7. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Stop-VM SEA-CORE1
   ```

8. Close the PowerShell sessions.

9.5 Exercise 2: Implementing backup and restore with Windows Server Backup

9.5.1 Scenario

You must evaluate Windows Server Backup for your member servers. You decided to configure Windows Server Backup of the **SEA-SVR1** server and to perform a trial backup to the network share on **SEA-ADM1**.

The main tasks for this exercise are to:

1. Configure Windows Server Backup on **SEA-SVR1**.
2. Perform a backup to the network share on **SEA-ADM1**.

9.5.2 Task 1: Configure Windows Server Backup options

1. Use File Explorer to create a **C:\BackupShare** folder on **SEA-ADM1**. Share the folder so that **Authenticated Users** have Read/Write permissions.
2. In PowerShell, create a new remote PowerShell session to **sea-svr1.contoso.com**. Use **Contoso\Administrator** credentials to connect to the remote PowerShell on **SEA-SVR1**.
3. Use the **Install-WindowsFeature** cmdlet to install the **Windows-Server-Backup** feature on **SEA-SVR1**.
4. Use the **wbadmin /?** and **Get-Command** commands to get a list of the available commands for Windows Server Backup.

9.5.3 Task 2: Perform a backup

1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following commands, and then select Enter:

   ```
   $Policy = New-WBPolicy

   $Filespec = New-WBFileSpec -FileSpec "C:\Files"
   ```

2. After running the commands from the previous step, where you defined the variables for the backup policy and the file path to the backup, add this to the backup policy by entering the following command, and then selecting Enter:

   ```
   Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec
   ```

3. Now, you must configure a backup location on the **SEA-AD1** network share by entering the following commands, and then selecting Enter:

   ```
   $Cred = Get-Credential
   $NetworkBackupLocation = New-WBBackupTarget -NetworkPath "\\SEA-ADM1\BackupShare" -Credential $Cre
   ```

   > **Note:** When you receive the sign-in prompt, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

4. Now you must add this backup location to the backup policy by entering the following command, and then selecting Enter (if prompted, enter Y, and then select Enter):

   ```
   Add-WBBackupTarget -Policy $Policy -Target $NetworkBackupLocation
   ```

5. Before starting a backup job, you must configure more options to enable Volume Shadow Copy Service backup by entering the following command, and then selecting Enter:

   ```
   Set-WBVssBackupOptions -Policy $Policy -VssCopyBackup
   ```

6. To start a backup job, in order to back up the content of the **C:\Files** folder on **SEA-SVR1** to a network share on **SEA-ADM1**, you must enter the following command, and then select Enter:

   ```
   Start-WBBackup -Policy $Policy
   ```

   Wait until you receive a "The backup operation completed" message.

7. On **SEA-ADM1**, open File Explorer, and then browse to **C:\BackupShare**. Open the folder, and then ensure that the backup files are there.

9.6 lab: title: 'Lab: Configuring security in Windows Server' module: 'Module 8: Windows Server security'

10 Lab: Configuring security in Windows Server

10.1 Scenario

Contoso Pharmaceuticals is a medical research company with about 5,000 employees worldwide. They have specific needs for ensuring that medical records and data remain private. The company has a headquarters location and multiple worldwide sites. Contoso has recently deployed a Windows Server and Windows client infrastructure. You have been asked to implement improvements in the server security configuration.

10.2 Objectives

After completing this lab, you will be able to:

- Configure Windows Defender Credential Guard.
- Locate problematic user accounts.
- Implement and verify LAPS (Local Administrator Password Solution)

10.3 Estimate time: 40 minutes

10.4 Lab setup

Virtual machines: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-SVR1**, and **WS-011T00A-SEA-ADM1** User name: Contoso\Administrator Password: Pa55w.rd

10.5 Exercise 1: Configuring Windows Defender Credential Guard

10.5.1 Scenario

You decide to implement Windows Defender Credential Guard on the servers and administrative workstations to protect against Pass-the-Hash and Pass-the-Ticket credential thefts. You will use Group Policy to enable Credential Guard on your existing servers. For all new servers, you will use the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool to enable Credential Guard before the new servers are domain joined.

In this lab, you will set up the Group Policy and run the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool on an existing server.

> **Note**: In the lab environment, Credential Guard will not run VMs because they don't meet the requirements. You can still create the GPO (Group Policy Objects) and run the tool.

The main tasks for this exercise are to:

1. Enable Windows Defender Credential Guard using Group Policy.
2. Enable Windows Defender Credential Guard using the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool.

10.5.2 Task 1: Enable Windows Defender Credential Guard using Group Policy

1. Sign-in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start**, and then enter **Group Policy Management**.
3. Select **Group Policy Management**.
4. In the Group Policy Management Console, expand **Forest: `Contoso.com`**, expand **Domains**, expand `Contoso.com`, right-click or access the context menu for the **IT** OU (Organizational Unit), and then select **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** dialog box, in the **Name** text box, enter **CredentialGuard_GPO**, and then select **OK**.
6. In the **Group Policy Management** window, under **IT**, right-click or access the context menu for **CredentialGuard_GPO**, and then select **Edit**.
7. In the Group Policy Management Editor, navigate to **Computer Configuration\Policies\Administrative Templates\System\Device Guard**.
8. Select **Turn On Virtualization Based Security**, and then select the **policy setting** link.
9. Select **Enabled**.
10. In the **Select Platform Security Level** drop-down list, select **Secure Boot and DMA Protection**.
11. In the **Credential Guard Configuration** drop-down list, select **Enabled with UEFI lock**.
12. In the **Secure Launch Configuration** drop-down list, select **Enabled**, and then select **OK**.
13. Close the Group Policy Management Editor.
14. Close the Group Policy Management Console.

10.5.3 Task 2: Enable Windows Defender Credential Guard using the hypervisor-protected code integrity and Windows Defender Credential Guard hardware readiness tool

1. On **SEA-ADM1**, select **Start**, and then enter **Powershell**.
2. Right-click or access the context menu for **Windows PowerShell**, and then select **Run as administrator**.
3. Navigate to **c:\labfiles\Mod08**.
4. Enter the following command:

   ```
   DG_Readiness_Tool.ps1 -Enable -AutoReboot
   ```

5. Your virtual machine will restart after the tool has completed running.
6. When the virtual machine restarts, reenter the credentials for **Contoso\Administrator**.

10.5.4 Results

After completing this exercise, you will have:

1. Used Group Policy to implement Windows Defender Credential Guard on all computers in your organization.

2. Enabled Windows Defender Credential guard immediately on your local computer.

10.6 Exercise 2: Locating problematic accounts

10.6.1 Scenario

You want to check whether your organization has user accounts with passwords that are configured not to expire and remediate this setting. You also want to check which accounts haven't signed in for 90 of days or more and disable them.

The main tasks for this exercise are to:

1. Locate and reconfigure accounts with passwords that don't expire.
2. Locate and disable accounts to which no sign-ins have occurred for at least 90 days.

10.6.2 Task 1: Locate and reconfigure accounts with passwords that don't expire

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Open Windows PowerShell.
3. Enter the following command:

```
Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true}
```

4. Review the list of user accounts returned.
5. Enter the following command:

```
Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true} | Set-ADUser -PasswordN
```

6. Rerun the command from step 3 and notice that no users are returned.

10.6.3 Task 2: Locate and disable accounts to which no sign-ins have occurred for at least 90 days

1. Enter the following commands:

```
$days = (Get-Date).Adddays(-90)
Get-ADUser -Filter {LastLogonTimeStamp -lt $days -and enabled -eq $true} -Properties LastLogonTime
```

2. In the lab environment, no accounts will be returned.
3. Enter the following command:

```
Get-ADUser -Filter {LastLogonTimeStamp -lt $days -and enabled -eq $true} -Properties LastLogonTime
```

4. No results will be returned in the lab environment.

10.7 Exercise 3: Implementing LAPS

10.7.1 Scenario

At present, the same local administrator account password is used across all servers and workstations at Contoso. To remedy this problem, you will configure and deploy LAPs.

The main tasks for this exercise are:

1. Prepare OU and computer accounts for LAPS.
2. Prepare AD DS (Active Directory) for LAPS.
3. Deploy LAPS client-side extension.
4. Verify LAPS.

10.7.2 Task 1: Prepare OU and computer accounts for LAPS

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Open Windows PowerShell.
3. Enter the following commands:

```
New-ADOrganizationalUnit -Name "Seattle_Servers"
Get-ADComputer SEA-SVR1 | Move-ADObject -TargetPath "OU=Seattle_Servers,DC=Contoso,DC=com"
```

4. Enter the following command:

   ```
   Msiexec /I C:\Labfiles\Mod08\LAPS.x64.msi
   ```

5. When the **Local Administrator Password Solution Setup Wizard** opens, select **Next**.
6. Select **I accept the terms in the License Agreement**, and then select **Next**.
7. Under **Custom Setup**, in the drop-down menu next to **Management Tools**, select **Entire feature will be installed on the local hard drive**.
8. Select **Next**, select **Install**, and then select **Finish**.

10.7.3 Task 2: Prepare AD DS for LAPS

1. In Windows PowerShell, enter the following commands:

   ```
   Import-Module admpwd.ps
   Update-AdmPwdADSchema
   Set-AdmPwdComputerSelfPermission -Identity "Seattle_Servers"
   ```

2. Select **Start**, and then enter **Group Policy**.
3. Select **Group Policy Management**.
4. In the Group Policy Management Console, expand **Forest: `Contoso.com`**, expand **Domains**, expand `Contoso.com`, right-click or access the context menu for the **Seattle_Servers** OU, and then select **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** dialog box, in the **Name** text box, enter **LAPS_GPO**, and then select **OK**.
6. In the **Group Policy Management** window, under **Seattle_Servers**, right-click or access the context menu for **LAPS_GPO**, and then select **Edit**.
7. In the **Group Policy Management Editor** window, under **Computer Configuration**, expand the **Policies** node, expand the **Administrative Templates** node, and then select **LAPS**.
8. Select the **Enable local admin password management** policy, and then select the **policy settings** link.
9. In the **Enable local admin password management** window, select **Enabled**, and then select **OK**.
10. Select the **Password Settings** policy, and then select the **policy settings** link.
11. In the **Password Settings** policy dialog box, select **Enabled**, and then configure **Password Length** to **20**.
12. Verify that the **Password Age (Days)** is configured to **30**, and then select **OK**.
13. Close the Group Policy Management Editor.

10.7.4 Task 3: Deploy LAPS client-side extension

1. Switch to **SEA-SVR1**, using **Contoso\Administrator** with the password **Pa55w.rd**.

   Note: You will be prompted to change your password, due to the previous exercise. Use the new password in place of the documented password throughout the remainder of the lab.

2. Enter the following command:

   ```
   Msiexec /I \\SEA-ADM1\c$\Labfiles\Mod08\LAPS.x64.msi
   ```

3. When the **Local Administrator Password Solution Setup Wizard** opens, select **Next**.
4. Select **I accept the terms in the License Agreement**, and then select **Next**.
5. Select **Next** again, and then select **Install**.
6. Select **Finish**.
7. Enter the following command:

```
gpupdate /force
```

10.7.5 Task 4: Verify LAPS

1. Switch to **SEA-ADM1**.
2. Select **Start**, select **LAPS**, and then select **LAPS UI**.
3. In the **LAPS UI** dialog box, in the **ComputerName** text box, enter **SEA-SVR1**, and then select **Search**.
4. Review the **Password** and the **Password expires** values, and then select **Exit**.
5. In the Windows PowerShell window, enter the following command:

   ```
   Get-ADComputer SEA-SVR1 -Properties ms-Mcs-AdmPwd
   ```

6. Review the password assigned to SEA-SVR1.
7. Close the gridview window.

10.7.6 Results

After completing this lab, you will have:

- Prepared an OU and computer accounts for LAPs.
- Prepared your AD DS for LAPS.
- Deployed LAPS client-side extension.
- Verified that you implemented LAPS successfully.

10.8 lab: title: 'Lab: Implementing RDS in Windows Server' module: 'Module 9: RDS in Windows Server'

11 Lab: Implementing RDS in Windows Server

11.1 Scenario

You have been asked to configure a basic Remote Desktop Services (RDS) environment as the starting point for the new infrastructure that will host the sales application. You would like to deploy RDS services, perform initial configuration, and demonstrate to the delivery team how to connect to an RDS deployment.

You are evaluating whether to use user profile disks for storing user profiles and making the disks available on all servers in the collection. A coworker reminded you that users often store unnecessary files in their profiles, and you need to explore how to exclude such data from the profile and set a limit on the profile size.

As the sales application will publish on the RD Web Access site, you also have to learn how to configure and access RemoteApp programs from the Remote Desktop Web Access (RD Web Access) portal.

You been tasked with creating a proof of concept (POC) for a virtual machine (VM)—based session deployment of Virtual Desktop Infrastructure (VDI). You will create a virtual desktop template on a preexisting Microsoft Hyper-V VM manually with a few optimizations.

11.2 Objectives

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

- Implement RDS
- Configure session collection settings and use RDS
- Configure virtual desktop template

11.3 Lab Setup

Estimated Time: 90 minutes

For this lab, you'll use the following VMs:

- **WS-011T00A-SEA-DC1**

- **WS-011T00A-SEA-RDS1**
- **WS-011T00A-SEA-CL1**

User Name: Contoso\Administrator

Password: Pa55w.rd

Sign in to **WS-011T00A-SEA-DC1** and **WS-011T00A-SEA-RDS1** by using the following credentials:

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

Sign in to **WS-011T00A-SEA-CL1** by using the following credentials:

- User name: **Jane**
- Password: **Pa55w.rd**
- Domain: **Contoso**

11.3.1 Exercise 1: Implementing RDS

11.3.2 Scenario

In this exercise, you will learn how to install RDS using Windows PowerShell and Server Manager. You will create a session collection using Windows PowerShell, and then change various collection settings. You will configure User Profile Disk using both Windows PowerShell and graphical user interfaces (GUIs), and connect to a Remote Desktop Session Host (RD Session Host) using the Remote Desktop Web (RD Web) portal. You will conclude the exercise by verify that a User Profile Disk has been created for a user.

The main tasks for this exercise are as follows:

1. Install RDS.
2. Create a session collection.
3. Configure the session collection properties.
4. Connect to the session collection from the RD Web portal

11.3.2.1 Task 1: Install RDS

11.3.2.1.1 Install RDS using Server Manager

1. On **SEA-RDS1**, open **Server Manager**, and then select **Manage**.
2. Select **Add Roles and Features**, and in the **Add Roles and Features Wizard**, select **Next**.
3. On the **Select installation type** page, select **Remote Desktop Services installation**, and then select **Next**.
4. On the **Select deployment type** page, select **Next**.

   NOTE: Even though, we could have selected the **Quick Start** deployment option and have all three required RDS role services installed on **SEA-RDS1**, you selected the **Standard deployment** option to practice selecting different servers for the RDS role services. Furthermore, the **Quick Start** deployment option will create a collection named **QuickSessionCollection** and publish the following RemoteApp Programs: **Calculator**, **Paint**, and **WordPad**.

4. On the **Select deployment scenario** page, select **Session-based desktop deployment**, and then select **Next**.
5. On the **Review role services** page, select **Next**.
6. On the **Specify RD Connection Broker server** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`, and then select **Next**.
7. On the **Specify RD Web Access server** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com` and then select **Next**.
8. On the **Specify RD Session Host servers** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`, and then select **Next**.
9. On the **Confirm selections** page, select **Cancel**.

11.3.2.1.2 Install RDS using Windows PowerShell

NOTE: We will now do the actual installation of RDS using Windows PowerShell. The previous steps were included to demonstrate how to install RDS using Server Manager.

1. Switch to **SEA-DC1**.
2. In the **Administrator: C:\Windows\system32\cmd.exe** command prompt window, enter the following command, and then select Enter: `powershell`
3. In the command prompt window, enter the following command, and then select Enter: `$SVR="SEA-RDS1.contoso.com"`
4. In the command prompt window, enter the following command, and then select Enter: `New-RDSessionDeployment -ConnectionBroker $SVR -WebAccessServer $SVR -SessionHost $SVR`
5. Wait for the installation to complete, which will take approximately 5 minutes, and then wait as **SEA-RDS1** restarts automatically.
6. Switch to **SEA-RDS1**, and sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
7. Open **Server Manager**, and wait for it to refresh.
8. In **Server Manager**, select **Remote Desktop Services**.

11.3.2.2 Task 2: Create a session collection

11.3.2.2.1 Create and configure a session collection using Server Manager

NOTE: RDS in Windows Server supports two types of Session Collections on a single RD Session Host: an RD Session Collection, or a RemoteApp Session Collection. You cannot run both session collection types on the same RD Session Host by default. Therefore, when you're doing this exercise, you will first create an RD Session Host collection and verify that it works and then create a RemoteApp Session collection and verify that as well.

1. On **SEA-RDS1**, on the **Remote Desktop Service Overview** page, select **Collections**.
2. Under **COLLECTIONS**, select **TASKS**, and then select **Create Session Collection**. You might need to scroll to access this option.
3. On the **Before you begin** page, select **Next**.
4. On the **Name the collection** page, in the **Name** field, enter **IT**, and then select **Next**.
5. On the **Specify RD Session Host servers** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`, and then select **Next**.
6. On the **Specify user groups** page, remove **CONTOSO\Domain Users**, and then select **Add**. Add the **CONTOSO\IT** group and then select **OK**. Verify that **CONTOSO\IT** is listed under **User Groups**, and then select **Next**.
7. On the **Specify user profile disks** page, clear the **Enable user profile disks** check box, and then select **Next**.
8. On the **Confirm selections** page, select **Cancel**.
9. When prompted, select **Yes**.
10. Minimize **Server Manager**.

11.3.2.2.2 Create and configure a session collection using Windows PowerShell

NOTE: We will now create and configure the session collection using Windows PowerShell. The previous steps were included to demonstrate how to create a session collection using Server Manager.

1. On **SEA-RDS1**, open Windows PowerShell.
2. At the command prompt, enter the following command, and then select Enter: `New-RDSessionCollection -CollectionName IT -SessionHost SEA-RDS1.Contoso.com -CollectionDescription "This Collection is for the IT department in Contoso" -ConnectionBroker SEA-RDS1.Contoso.com`
3. Wait for the command to complete, which will take approximately 1 minute.
4. Maximize **Server Manager**, and then select **Overview**.
5. Refresh **Server Manager** by selecting the **F5** key.
6. In **Server Manager**, select **Collections**, and verify that a collection named **IT** is in the details pane.

11.3.2.3 Task 3: Configure the Session Collection properties

11.3.2.3.1 Configure device redirection settings

1. On SEA-RDS1, select the **IT** collection. Next to **PROPERTIES**, select **TASKS**, and then select **Edit Properties**.
2. On the **Session Collection** page, select the various settings and notice how the collection is configured.
3. select **Client Settings**, and verify that **Audio and video playback** and **Audio recording** is enabled.
4. select **User Profile Disks**, and verify that **User Profiles Disks** is not enabled.

5. In the **IT Properties** dialog box, select **Cancel**.
6. Minimize **Server Manager**.
7. In the Windows PowerShell window, enter the following command, and then select Enter:`Get-RDSessionCollectionCon -CollectionName IT -Client | Format-List`
8. Examine the output and notice that next to **ClientDeviceRedirectionOptions**, the following entries are listed:
   - **AudioVideoPlayBack**
   - **AudioRecording**
   - **PlugAndPlayDevice**
   - **SmartCard**
   - **Clipboard**
   - **LPTPort**
   - **Drive**
9. In the WindowsPowerShell window, enter the following command, and then select Enter:`Set-RDSessionCollectionCon -CollectionName IT -ClientDeviceRedirectionOptions PlugAndPlayDevice, SmartCard,Clipboard,LPTPort,`
10. In the WindowsPowerShell window, enter the following command, and then select Enter:`Get-RDSessionCollectionCon -CollectionName IT -Client | Format-List`
11. Examine the output and notice that next to **ClientDeviceRedirectionOptions**, only the following entries are listed now:
    - **PlugAndPlayDevice**
    - **SmartCard**
    - **Clipboard**
    - **LPTPort**
    - **Drive**

11.3.2.3.2 Configure User Profile Disks for IT collection

1. Switch to **SEA-DC1**, and in the command prompt window, enter the following commands, one line at a time, and then select Enter:

- `New-Item C:\RDSUserProfiles -itemtype directory`
- `New-SMBShare -Name "RDSUserProfiles" -Path "C:\RDSUserProfiles" -FullAccess "Contoso\SEA-RDS1$", "Contoso\administrator"`
- `$acl = Get-Acl C:\RDSUserProfiles`
- `$AccessRule = New-Object System.Security.AccessControl.FileSystemAccessRule("Contoso\SEA-RDS1$","F`
- `$acl.SetAccessRule($AccessRule)`
- `$acl | Set-Acl C:\RDSUserProfiles`

2. Verify that each command executes successfully.
3. Switch to **SEA-RDS1**, and select the **IT** collection.
4. Next to **PROPERTIES**, select **TASKS**, and then select **Edit Properties**.
5. On the **Session Collection** page, select **User Profile Disks**, and then select **Enable user profile disks**.
6. In the **Location** field, enter **\\SEA-DC1\RDSUserProfiles**. In the **Maximum size (in GB)**, enter **10**, and then select **OK**.

11.3.2.4 Task 4: Connect to the Session Collection from RD Web portal

1. On **SEA-CL1**, Open **Microsoft Edge**.
2. In Microsoft Edge, browse to `https://SEA-RDS1.Contoso.com/rdweb`.
3. On the **This site is not secure** page, select **Details**, and then select **Go on to the webpage**.

   NOTE: This page opens because RD Web is using a self-signed certificate that is not trusted by the client. In a real production deployment, you would use trusted certificates.

4. On the **RD Web Access** page, sign-in using **contoso\jane** as the user name, and password as **Password**. If prompted by **Microsoft Edge** to save the password, select **Never**.
5. On the **RD Web Access** page, under **Current folder: /**, select **IT**, and when prompted, select **Open**.
6. In the **Remote Desktop Connection** dialog box, select **Connect**.

NOTE: This prompts the **Unknown publisher** pop up window because certificates for RDS have not yet been configured.

7. In the **Windows Security** dialog box, use **Pa55w.rd** as the password, and then select Enter.
8. After the connection completes, on **SEA-RDS1**, sign out of the session.
9. Sign out of the RD Web portal and close **Microsoft Edge**.

11.3.2.4.1 Verify User Profile Disk creation

1. Switch to **SEA-DC1**, and in the command prompt window, enter the following command, and then select Enter: `cd\`
2. Enter the following command, and then select Enter: `cd RDSUserProfiles`
3. Enter the following command, and then select Enter: `dir`
4. Examine the contents of the **RDSUserProfiles** folder. Verify that there is a **.vhdx** file with an SID (a long string that starts with **S-1-5-21**) in its name.

11.3.3 Exercise 2: Configuring RemoteApp collection settings

11.3.4 Scenario

In this exercise, you will explore how to add RemoteApp Programs to RDS using both Server Manager and Windows PowerShell. You will then run a RemoteApp Program from the RD Web portal.

The main tasks for this exercise are as follows:

1. Create and configure a RemoteApp collection using Server Manager
2. Create and configure a RemoteApp program using Windows PowerShell.
3. Run RemoteApp from RD Web portal.

11.3.4.1 Task 1: Create and configure a RemoteApp collection using Server Manager

1. Switch to **SEA-RDS1**.
2. In **Server Manager**, next to **REMOTEAPP PROGRAMS**, select **TASKS**, and then select **Publish RemoteApp Programs**.
3. On the **Select RemoteApp programs** page, select **WordPad** from the list, and then select **Next**.
4. On the **Confirmation** page, select **Publish**, and then wait for the RemoteApp to be published.
5. Verify that **WordPad** is listed in the details pane under **RemoteApp Program**, and then select **Close**.

11.3.4.2 Task 2: Create and configure a RemoteApp program using Windows PowerShell

1. ON **SEA-RDS1**, right-click or access the context menu for **Start**, and then select **Windows PowerShell.**
2. At the Windows PowerShell command prompt, enter the following command, and then select Enter:
```
New-RDRemoteApp -Alias Paint -DisplayName Paint -FilePath "C:\Windows\system32\mspaint.exe"
-ShowInWebAccess 1 -collectionname IT -ConnectionBroker SEA-RDS1.Contoso.com
```
3. Enter the following command, and then select Enter: `Get-RDRemoteApp -CollectionName IT`
4. Examine the output of the command. Notice that you will get a list of all published RemoteApp Programs.
5. Maximize **Server Manager**, and then select **Overview**.
6. Refresh **Server Manager** by selecting **F5**.
7. In **Server Manager**, select the **IT** collection and verify that **Paint** is listed in the details pane under **REMOTEAPP PROGRAMS**.

11.3.4.3 Task 3: Run RemoteApp from RD Web portal

1. On **SEA-CL1**, open **Microsoft Edge**, and brwose to `https://SEA-RDS1.Contoso.com/rdweb`.
2. On the **This site is not secure page**, select **Details**, and then select **Go on to the webpage**.

   NOTE: This page opens because RD Web is using a self-signed certificate that is not trusted by the client. In a real production deployment, you would use trusted certificates.

3. On the **RD Web Access** page, sign-in as **contoso\jane** using **Pa55w.rd** as the password.
4. On the **RD Web Access** page, run **Paint**, and when prompted, select **Open**.
5. In the **Remote Desktop Connection** dialog box, select **Connect**.

   NOTE: The **Unknown publisher** pop-up window displays because you have not yet configured certificates for RDS.

6. In the **Windows Security** dialog box, use **Pa55w.rd** as the password.
7. Wait for the **Paint** RemoteApp program to start, and then test its functionality.
8. Close **Paint**.
9. Back in the RD Web portal**RD Web, sign out.
10. Close Microsoft Edge.

11.3.5 Exercise 3: Configure a virtual desktop template

11.3.6 Scenario

In this exercise, you will explore how to manually configure a virtual desktop template. The Hyper-V VM, you are using has already been created.

The main tasks for this exercise are as follows:

1. Verify the operating system (OS) version.
2. Disable unnecessary services.
3. Disable unnecessary scheduled tasks.
4. Prepare the virtual desktop template by using System Preparation Tool (Sysprep).

11.3.6.1 Task 1: Verify the OS version

1. On **SEA-CL1**, sign in as **.\Admin** with the password **Pa55w.rd**.
2. On **SEA-CL1**, and then open **About your pc**.
3. In the **Settings** app, on the **About screen**, verify the following information:

- The Windows operating system edition is Windows 10 Enterprise
- The System type is 64-bit OS

4. Close the **Settings** app.

11.3.6.2 Task 2: Disable unnecessary services

1. On **SEA-CL1**, and then open **Services**.
2. In the **Services** window, right-click or access the context menu for **Background Intelligent Transfer Service**.
3. In the **Background Intelligent Transfer Service Properties (Local Computer)** dialog box, on the **General** tab, select **Stop**.
4. In the **Startup type** box, select **Disabled**, and then select **OK**.
5. Repeat steps 2 through 4 for the following services:

- **Diagnostic Policy Service**
- **Shell Hardware Detection**
- **Volume Shadow Copy**
- **Windows Search**

5. Close the **Services** window.

11.3.6.3 Task 3: Disable unnecessary scheduled tasks

1. On **SEA-CL1**, and then open **Task Scheduler**.
2. In **Task Scheduler**, expand **Task Scheduler Library**, expand **Microsoft**, expand **Windows**, and then select **Defrag**.
3. Disable **ScheduledDefrag**, and then close the **Task Scheduler** window.

11.3.6.4 Task 4: Prepare the virtual desktop template by using Sysprep

1. On **SEA-CL1**, browse to **C:\Windows\System32\Sysprep**, and then run **sysprep.exe**.
2. In the **System Preparation tool 3.14** dialog box, in the **System Cleanup Action** box, select **Enter System Out-of-Box Experience (OOBE)**, and then select the **Generalize** check box.
3. In the **Shutdown Options** box, select **Shutdown**, and then select **OK**.
4. Wait while Sysprep completes and shuts down the VM.

11.4 After completing this exercise, you will have prepared a Hyper-V VM to be a virtual desktop template.

11.5 lab: title: 'Lab: Deploying network workloads' module: 'Module 10: Remote Access and web services in Windows Server'

12 Lab: Deploying network workloads

12.1 Scenario

The employees in the IT department at Contoso need to be able to access server systems outside of business hours to correct issues that arise during weekends or holidays. Some of the employees are using computers that aren't members of the `contoso.com` domain. Other users are running non-Windows operating systems on their computers. To enable remote access for these users, you will provide remote access to Windows Admin Center and secure it with Web Application Proxy and deploy a secure VPN solution using the SSTP VPN protocol.

You are a web server administrator for Contoso and your company is preparing to deploy a new intranet web application on an internal web server. You need to verify the server configuration and install IIS. The website must be accessible using a friendly DNS name and all web connections to and from the server must be encrypted.

12.2 Objectives

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

- Deploy and configure Web Application Proxy
- Implement a VPN (virtual private network) solution
- Deploy and configure a web server

12.3 Lab setup

Estimated time: 60 minutes

For this lab, you will use the following virtual machines:

- **WS-011T00A-SEA-DC1**
- **WS-011T00A-SEA-ADM1**
- **WS-011T00A-SEA-SVR1**
- **WS-011T00A-SEA-SVR3**
- **WS-011T00A-SEA-CL1**

Sign in by using the following credentials:

- User Name: **Contoso\Administrator**
- Password: **Pa55w.rd**

12.4 Exercise 1: Implementing Web Application Proxy

Contoso has decided to make Windows Admin Center available remotely to administrators. To secure Windows Admin Center, you need to deploy Web Application Proxy. For initial testing, you will use pass-through preauthentication. AD FS is being installed on **SEA-SVR1** and Web Application Proxy is being installed on **SEA-SVR3**. Certificates are already installed on both servers in preparation for the installation.

The main tasks for this exercise are as follows:

1. Install AD FS on **SEA-SVR1**.
2. Create DNS entries for AD FS and Web Application Proxy.
3. Install Remote Access management tools.
4. Install Web Application Proxy.
5. Configure Web Application Proxy.
6. Configure a web application.
7. Configure Windows Defender Firewall to allow remote access
8. Test the web application.

12.4.1 Task 1: Install AD FS on SEA-SVR1

1. On **SEA-SVR1**, at the command prompt, run **powershell.exe**.
2. At the Windows PowerShell prompt, run **C:\Labfiles\Mod03\InstallADFS.ps1**.

12.4.2 Task 2: Create DNS entries for AD FS and Web Application proxy

1. On **SEA-ADM1**, in Windows Admin Center, connect to **SEA-DC1**.
2. Use DNS to create two new host records in `Contoso.com`:
   - **remoteapp** resolves to: **172.16.10.14 (SEA-SVR3)**.
   - **fs** resolves to: **172.16.10.12 (SEA-SVR1)**.

12.4.3 Task 3: Install Remote Access management tools

1. On **SEA-ADM1**, in **Windows Admin Center**, connect to **SEA-ADM1**.
2. Use **Roles and features** to install **Remote Access Management Tools** in Remote Server Administration Tools.

12.4.4 Task 4: Install Web Application Proxy

1. On **SEA-ADM1**, in **Windows Admin Center**, connect to **SEA-SVR3**.
2. Use **Roles & features** to install the **Web Application Proxy** role service in the **Remote Access** role.

12.4.5 Task 5: Configure Web Application Proxy

1. On **SEA-ADM1**, in **Server Manager**, open **Remote Access Management**.
2. In **Remote Access Management Console**, use the **Manage a Remote Server** option to connect to **SEA-SVR3**.
3. Use the **Web Application Proxy Wizard** to configure **Web Application Proxy** with following settings:
   - Federation service name: `fs.Contoso.com`
   - User name: **Contoso\Administrator**
   - Password: **Pa55w.rd**
   - Certificate: `fs.contoso.com`

   Note: If you get an error in **Remote Access Management Console** indicating that cmdlets are not found, restart **Remote Access Management Console**.

12.4.6 Task 6: Configure a web application

1. On **SEA-ADM1**, in **Remote Access Management Console**, publish a web application with the following settings:

   - Pre-authentication: **Pass-through**
   - Name: **RemoteApp**
   - External URL: `https://remoteapp.contoso.com`
   - External certificate: `remoteapp.contoso.com`
   - Backend server URL: `https://SEA-ADM1.contoso.com`

   Note: You will receive a warning that the external URL and backend URL are different. You can ignore this warning.

12.4.7 Task 7: Configure Windows Defender Firewall to allow remote access

1. On **SEA-ADM1**, in **Windows Admin Center**, connect to **SEA-ADM1**.
2. Use **Firewall** to create a new firewall rule with the following settings:
   - Name: **SecureWeb**
   - Direction: **Incoming**
   - Action: **Allowed**
   - Enable firewall rule: **Yes**
   - Protocol: **TCP**
   - Local port: **443**
   - Remote port: **blank**
   - ICMP types: **blank**
   - Profiles: **Select All**

12.4.8 Task 8: Test the web application

1. On **SEA-CL1**, open **Microsoft Edge** and connect to `https://remoteapp.contoso.com`.
2. In **Microsoft Edge**, sign in as **Contoso\Administrator** with the password **Pa55.wrd**.

12.4.9 Exercise 2: Implementing VPN in Windows Server

12.4.10 Scenario

The first step to implementing VPN is to verify and configure certificate requirements for a SSTP (Secure Socket Tunneling Protocol) VPN. You then must configure the Remote Access server to provide VPN connectivity, and you also must create a remote access policy to ensure that the clients can connect to the server by using the SSTP VPN protocol.

The main tasks for this exercise are as follows:

1. Configure RRAS service and NPS policies for VPN
2. Configure a client VPN connection
3. Test the VPN connection

12.4.10.1 Task 1: Configure RRAS service and NPS policies for VPN

1. On **SEA-ADM1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:

```
Install-WindowsFeature -name RemoteAccess,Routing -IncludeManagementTools
```

Wait for the command to complete, which should take approximately 1 minute.

12.4.10.1.1 Request certificate for SEA-ADM1

1. On **SEA-ADM1**, In the PowerShell window, enter the following command, and then select Enter: `mmc`
2. Add the **Certificates** snap-in for the computer account and local computer.
3. In the **Certificates snap-in** console tree, navigate to **Certificates (local)\Personal**, and then request a new certificate.
4. Under **Request Certificates**, configure the **Contoso Web Server** certificate with the following setting:
   - Subject name: Under `Common name`, enter `vpn.contoso.com`
   - Friendly name: **Contoso VPN**
5. In the Certificates snap-in, expand **Personal** and select **Certificates**, and then, in the **details** pane, verify that a new certificate with the name `vpn.contoso.com` is enrolled with **Intended Purposes** of **Server Authentication**.
6. Close the **Microsoft Management Console (MMC)**. When you receive a prompt to save the settings, select **No**.

12.4.10.1.2 Change the HTTPS bindings

1. Open the **Internet Information Services (IIS) Manager console**.
2. In **Internet Information Services (IIS) Manager**, navigate to **SEA-ADM1/Sites**, and then select **Default Web site**.
3. Configure site bindings by selecting **Contoso VPN** as SSL Certificate. When prompted, select **Yes**.
4. Close the **Internet Information Services (IIS) Manager** console.

12.4.10.1.3 Configure and enable VPN configuration

1. On **SEA-ADM1**, open **Routing and Remote Access**.
2. Right-click **SEA-ADM1 (local)** or access the context menu, and then select **Configure and Enable Routing and Remote Access**.
3. On the **Welcome to Routing and Remote Access Server Setup Wizard**, select **Next**.
4. On the **Configuration** page, select **Custom configuration**, and then select **Next**.
5. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then select **Next**.
6. On the **Completing the Routing and Remote Access Server Setup Wizard** page, select **Finish**. When prompted, select **Start service**.

7. Expand **SEA-ADM1 (local)**, right-click (or access the context menu) **Ports**, and then select **Properties**.
8. Verify that **128** ports exist for **Wan Miniport (SSTP)**, **Wan Miniport (IKEv2)** and**Wan Miniport (L2TP)**. Modify the number of ports for each type of connection to **5**. Disable the use of **Wan Miniport (PPTP)**.
9. Close the **Ports Properties** dialog box, and when prompted, select **Yes**.
10. Right-click (or access the context menu) **SEA-ADM1 (local)**, and then select **Properties**.
11. On the **General** tab, verify that **IPv4 Remote access server** is selected.
12. On the **Security** tab, select the drop-down arrow next to **Certificate**, and then select `vpn-contoso.com`.
13. Select **Authentication Methods**, and then verify that **EAP** is selected as the authentication protocol.
14. On the **IPv4** tab, verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
15. To close the **SEA-ADM1 (local) Properties** dialog box, select **OK**, and then, when you receive a prompt, select **Yes**.

12.4.10.1.4 Configure the Remote Access policies

1. On **SEA-ADM1**, from **Server Manager**, open the **Network Policy Server** console.
2. In the **Network Policy Server** console, in the **navigation** pane, expand **Policies**, and then select **Network Policies**.
3. Create a new network policy by using the **New Network Policy Wizard** with the following settings:
   - Policy name: **Contoso IT VPN**
   - Type of network access server: **Remote Access Server(VPN-Dial up)**
   - Windows Groups: **IT**
   - Specify Access Permission: **Access granted**
   - Configure Authentication Methods:
     - Add **Microsoft Secured password (EAP-MSCHAP v2)**
     - **Add Microsoft: Smart Card or other certificate**
     - Clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box
4. Complete the **New Network Policy Wizard** by accepting the default settings on the other pages.
5. Close all open windows.

12.4.10.2 Task 2: Configure a client VPN connection

1. On **SEA-CL1**, right-click (or access the context menu) **Start**, and then select **Network Connections**.
2. In **Network & Internet**, select **VPN**, and then select **Add a VPN connection**.
3. In the **Add a VPN connection** wizard, use the following values and then select **Save**:
   - VPN provider: **Windows (built-in)**
   - Connection Name: **Contoso VPN**
   - Server name or address: `vpn.contoso.com`
   - VPN type: **Secure Socket Tunneling Protocol (SSTP)**
   - Type of sign-in info: **User name and password**
   - Remember my sign-in info: **Cleared**

12.4.10.3 Task 3: Test the VPN connection

1. In **Network & Internet**, select **Contoso VPN**, and then select **Connect**.
2. In the **Sign in** dialog box, in the **User name** field, enter **contoso\jane**, in the **Password** field, enter **Pa55w.rd**, and then select **OK**.
3. Verify that you are now connected to the VPN server.

12.4.10.3.1 Verify connection on client and VPN server

1. On **SEA-CL1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter: `Get-NetIPConfiguration`
2. Examine the output and verify that **Contoso VPN** is listed next to **InterfaceAlias**. Also verify that the **Contoso VPN** interface has been issued an IP Address. This is the IP address for VPN connection assigned by RRAS.
3. Switch to **SEA-ADM1** and maximize the **Routing and Remote Access** snap-in.

4. In the **Routing and Remote Access** snap-in, select **Remote Access Clients (0)** and verify that **Contoso\jane** is listed under the **User Name** column. This indicates that the user is connected to the VPN Server.
5. Maximize **Server Manager**, and in the **Tools** menu select **Remote Access Management**.
6. In the **Remote Access Management** Console, select **Remote Client Status** and verify that **CONTOSO\jane** is listed in the details pane under **Connected Clients**. Notice that the VPN protocol used is displayed under the **Protocol/Tunnel** field as **Sstp**.

Question: Why did you disable the PPTP authentication protocol when you configured the ports of the VPN Server?

Answer: The PPTP protocol is considered highly insecure and you shouldn't use it at all.

Results: After completing this exercise, you should have installed and configured the Remote Access server to successfully provide VPN access.

12.4.11 Exercise 3: Deploying and configuring web server

12.4.12 Scenario

In this exercise, you will install the web server role on an internal server. You will then verify the installation of IIS and configure remote management of IIS. You will then add an A record in DNS for the new website and enroll a web server certificate. You will then verify that you can reach the website using the new DNS name and that the connection to the website is encrypted using SSL.

The main tasks for this exercise are as follows:

1. Install the Web Server role
2. Configure Web Server options
3. Create and configure a new site
4. Verify site functionality

12.4.12.1 Task 1: Install the Web Server role

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter: `Install-WindowsFeature -name Web-Server -IncludeManagementTools` Wait for the command to complete, which should take approximately 1 minute.

12.4.12.1.1 Verify the Web Server installation

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-eventLog System -After (Get-Date).AddHours(-1)` Verify that no errors display in connection with the installation of IIS.
2. Still in a Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-eventLog Application -After (Get-Date).AddHours(-1)` Verify that only errors with word **License** display under the **Message** column.

12.4.12.1.2 Verify that the Windows Firewall rules for HTTP and HTTPS traffic are enabled

1. In a Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-NetFirewallProfile -Name Domain | Get-NetFirewallRule | where-Object {$_.DisplayName -like "World Wide Web*"}`
2. This will return information about two rules: one for HTTP and one for HTTPS. Verify that both rules are enabled and allow inbound traffic.

12.4.12.1.3 Test the default website

1. Switch to **SEA-ADM1** and open Microsoft Edge. In the address bar, enter `http://SEA-SVR1`
2. Verify that IIS displays the default webpage.
3. In the address bar, enter `http://172.16.10.12`
4. Verify that IIS displays the default webpage.

12.4.12.2 Task 2: Configure Web Server options

12.4.12.2.1 Configure DNS for the default website

1. On **SEA-ADM1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:`Add-DnsServerResourceRecordA -ComputerName SEA-DC1 -Name "www" -ZoneName "contoso.com" -AllowUpdateAny -IPv4Address "172.16.10.12"`
2. In the Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-DnsServerResourceRecord -ComputerName SEA-DC1 -ZoneName "contoso.com"`
3. Verify in the output that the A record you just created exists in the `contoso.com` DNS zone.

12.4.12.2.2 Test the website by using DNS names

1. On **SEA-ADM1**, open Microsoft Edge and in the address bar, enter **`http://www.contoso.com`**
2. Verify that IIS displays the default webpage.

12.4.12.2.3 Enable remote management of IIS using IIS Manager

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:`Install-WindowsFeature -Name Web-Mgmt-Service`. Wait for the command to complete, which should take approximately 1 minute.
2. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:`Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\WebManagement\Server' -Name EnableRemoteManagement -Value 1`
3. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:`Restart-Service wmsvc`

   Note: Setting this registry key to 1 will enable remote management of IIS. You must restart the **Web Management Service (wmsvc)** after changing the registry key.

4. Switch to **SEA-ADM1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:`Install-WindowsFeature -Name Web-Mgmt-Console,Web-Scripting-Tools`. Wait for the command to complete, which should take approximately 1 minute.

   Note: The output from this command will return **NoChangeNeeded** under the **Exit Code** column. This is because, you already installed the management tools during exercise 1. This step has been left here intentionally to show the complete process of enabling remote management of IIS.

5. Open **Internet Information Services (IIS) Manager** and display the **Start Page**.
6. On the **Start Page**, under **Connection tasks**, select **Connect to a server**. Use the following information to complete the wizard:
   - Server name: **SEA-SVR1**
   - User name: **contoso\administrator**
   - Password: **Pa55w.rd**
   - Connection name: **SEA-SVR1**
7. When prompted by the **Server Certificate Alert** dialog window, select **Connect**.
8. In the **Connections** pane, select **Start Page**. **Notice Recent connections**, **Connection tasks**, **Online resources**, and **IIS News**.
9. In the **Connections** pane, select **SEA-SVR1 (contoso\administrator)**. Notice the icons listed in the **Features View** pane. In the **Actions** pane, notice the list of **Manage Server** actions.
10. In the **Connections** pane, expand **SEA-SVR1 (contoso\administrator)**, and then select **Sites**. In the **Features View** pane, notice the **Name** of the listed website and its **Status**.
11. In the **Actions** pane, select **Set Website Defaults**. In the **Website Defaults** dialog box, notice the **Application Pool** setting. Select **Cancel**.
12. Leave **Internet Information Services (IIS) Manager** open.

12.4.12.3 Task 3: Create and configure a new site

12.4.12.3.1 Create a webpage in the Default Website

1. Switch to **SEA-SVR1**, create, and save a new webpage in **Notepad** using the following information:
   - File name: **Default.htm**
   - Location: **c:\inetpub\wwwroot**
   - Content:** Contoso intranet running on SEA-SVR1 **

2. In the menu bar, select **File**, and then select **Save As**. In the **Save As** dialog box, select **File name**, and then delete ***.txt**. In the **File** name box, enter **c:\inetpub\wwwroot\default.htm**. Select the **Save** button.
3. Close **Notepad**.

12.4.12.3.2 Request a new Web Server certificate

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-Certificate -Template ContosoWebServer -DnsName www.contoso.com -CertStoreLocation cert:\LocalMachine\My`.
2. Wait for the command to complete, which should take approximately 30 seconds. Verify that **Issued** is displayed under **Status**.

12.4.12.4 Task 4: Verify site functionality

1. Switch to **SEA-ADM1**, in the **Internet Information Services (IIS) Manager**, right-click (or access the context menu) **Default Web Site**, and then select **Edit Bindings**.
2. In the **Site Bindings** dialog box, select **Add** and under **type**, select **https**.
3. Under **SSL certificate**, select the certificate displayed with a GUID, select **OK** and then select **Close**. The GUID will be similar to: **35B56A0F8D0AC682579BA893524EDFC6EC8FBA83**.
4. On **SEA-ADM1**, open Microsoft Edge and in the address bar, enter `http://www.contoso.com`. Verify that the website displays. Notice that **Not secure** is displayed next to `www.contoso.com`.
5. In the address bar, enter `https://www.contoso.com`. Verify that the website displays. Notice that a padlock displays next to `www.contoso.com`. This means that the website is protected using SSL.

12.5 lab: title: 'Lab: Monitoring and troubleshooting Windows Server' module: 'Module 11: Monitoring, performance, and troubleshooting'

13 Lab: Monitoring and troubleshooting Windows Server

13.1 Scenario

Contoso, Ltd is a global engineering and manufacturing company with its head office in Seattle, Washington, in the United States. An IT office and datacenter are in Seattle to support the Seattle location and other locations. Contoso recently deployed a Windows Server 2019 server and client infrastructure.

Because the organization deployed new servers, it's important to establish a performance baseline with a typical load for these new servers. You've been asked to work on this project. Additionally, to make the process of monitoring and troubleshooting easier, you decided to perform centralized monitoring of event logs.

13.2 Objectives

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

- Establish a performance baseline.
- Identify the source of a performance problem.
- Review and configure centralized event logs.

13.3 Lab setup

Estimated time: **40 minutes**

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

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

13.4 Lab setup

1. Select **SEA-DC1**.
2. Sign in by using the following credentials:
    - User name: **Administrator**

- Password: **Pa55w.rd**
- Domain: **Contoso**

3. Repeat these steps for **SEA-ADM1** and **SEA-CL1**.

13.5 Exercise 1: Establishing a performance baseline

13.5.1 Scenario

In this exercise, you'll use **Performance Monitor** on the server and create a baseline by using typical performance counters.

The main tasks for this exercise are:

1. Create and start a data collector set
2. Create a typical workload on the server
3. Analyze the collected data

   Note: After starting the Data Collector Set, there might be a delay of 10 minutes for the results to appear.

13.5.2 Task 1: Create and start a data collector set

1. Switch to **SEA-ADM1**.
2. Open **Performance Monitor**.
3. Create a new **User Defined** data collector set by using the following information to complete the process:
   - Name: **SEA-ADM1 Performance**
   - Create: **Create manually (Advanced)**
   - Type of data: **Performance counter**
   - Select the following counters (using all default instances):
     - **Memory\Pages/sec**
     - **Network Interface\Bytes Total/sec**
     - **PhysicalDisk\% Disk Time**
     - **PhysicalDisk\Avg. Disk Queue Length**
     - **Processor\% Processor Time**
     - **System\Processor Queue Length**
   - Sample interval: **1** second
   - Where to store data: default value
4. Save and close the data collector set.
5. In **Performance Monitor**, in the results pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Start**.

13.5.3 Task 2: Create a typical workload on the server

1. Open a **Command Prompt** window, and then run the following commands by selecting Enter after each command:

```
Fsutil file createnew bigfile 104857600
Copy bigfile \\SEA-dc1\c$
Copy \\SEA-dc1\c$\bigfile bigfile2
Del bigfile*.*
Del \\SEA-dc1\c$\bigfile*.*
```

2. Don't close the **Command Prompt** window.

13.5.4 Task 3: Analyze the collected data

1. Switch to **Performance Monitor**.
2. Stop the **SEA-ADM1 Performance** data collector set.
3. In **Performance Monitor**, in the navigation pane, browse to **Reports**, **User Defined**, **SEA-ADM1**, **SEA-ADM1_DateTime-000001**, and then review the report data. Use the Report view.
4. Record the values that are listed in the report for later analysis. Recorded values include:
   - **Memory\Pages/sec**

- **Network Interface\Bytes Total/sec**
- **PhysicalDisk% Disk Time**
- **PhysicalDisk\Avg. Disk Queue Length**
- **Processor% Processor Time**
- **System\Processor Queue Length**

13.5.5 Results

After this exercise, you should have established a baseline for performance-comparison purposes.

13.6 Exercise 2: Identifying the source of a performance problem

13.6.1 Scenario

In this exercise, you'll simulate a load to represent the system in live usage, gather performance data by using your data collector set, and then determine the potential cause of the performance problem.

The main tasks for this exercise are:

1. Create additional workload on the server
2. Capture performance data by using a data collector set
3. Remove the workload, and then review the performance data

13.6.2 Task 1: Create additional workload on the server

1. On **SEA-ADM1**, open File Explorer.
2. Browse to the **C:\Labfiles\Mod11** folder.
3. On **SEA-ADM1**, run **CPUSTRES64**.
4. Configure the first highlighted task to run **BUSY (75%)**.

13.6.3 Task 2: Capture performance data by using a data collector set

1. Switch to **Performance Monitor**.
2. In **Performance Monitor**, browse to **Data Collector Sets**, **User Defined**, and then in the results pane, start the **SEA-ADM1 Performance** data collector set.
3. Wait a minute to allow the data capture to occur.

13.6.4 Task 3: Remove the workload, and then review the performance data

1. Close CPUSTRES64, and then close File Explorer.
2. Switch to **Performance Monitor**.
3. Stop the **SEA-ADM1 Performance** data collector set.
4. In **Performance Monitor**, in the navigation pane, browse to **Reports**, **User Defined**, **SEA-ADM1**, **SEA-ADM1_DateTime-000002**, and then review the report data. Record the following values:
   - **Memory\Pages/sec**
   - **Network Interface\Bytes Total/sec**
   - **PhysicalDisk% Disk Time**
   - **PhysicalDisk\Avg. Disk Queue Length**
   - **Processor% Processor Time**
   - **System\Processor Queue Length**

13.6.5 Results

After this exercise, you should have used performance tools to identify a potential performance bottleneck.

13.6.6 Exercise 3: Viewing and configuring centralized event logs

13.6.7 Scenario

In this exercise, you'll use **SEA-DC1** to collect event logs from **SEA-ADM1**. Specifically, you'll use this process to gather performance-related alerts from your network servers.

The main tasks for this exercise are:

1. Configure subscription prerequisites
2. Create a subscription

3. Configure a performance counter alert
4. Introduce additional workload on the server
5. Verify the results
6. Prepare for the next module

13.6.8 Task 1: Configure subscription prerequisites

1. Switch to **SEA-ADM1**.
2. At the command prompt, run **winrm quickconfig** to enable the administrative changes that are necessary on a source computer. As you can observe, the WinRM service is running and enabled for remote management already.
3. Add **SEA-CL1** to the local **Event Log Readers** group.
4. Switch to **SEA-CL1**.
5. Open a **Command Prompt** window, and then run **wecutil qc** to enable the administrative changes that are necessary on a collector computer.

13.6.9 Task 2: Create a subscription

1. Open **Event Viewer**.
2. Create a new subscription with the following properties:
   - Computers: **SEA-ADM1**
   - Name: **SEA-ADM1 Events**
   - Collector: **initiated**
   - Events: **Critical**, **Warning**, **Information**, **Verbose**, and **Error**
   - Logged: **Last 7 days**
   - Logs: **Applications and Services Logs / Microsoft / Windows / Diagnosis-PLA / Operational**

13.6.10 Task 3: Configure a performance counter alert

1. Switch to **SEA-ADM1**.
2. Open **Performance Monitor**.
3. Create a new **User Defined** data collector set by using the following information to complete the process:
   - Name: **SEA-ADM1 Alert**
   - Create: **Create manually (Advanced)**
   - Type of data: **Performance counter Alert**
   - Select the following counters: **Processor% Processor Time** above **10** percent
   - Sample interval: **1** second
   - Where to store data: default value
   - Alert action: **Log an entry in the application event log**
4. Start the **SEA-ADM1 Alert** data collector set.

13.6.11 Task 4: Introduce additional workload on the server

1. On **SEA-ADM1**, open File Explorer.
2. Browse to the **C:\Labfiles\Mod11** folder.
3. On **SEA-ADM1**, run **CPUSTRES64**.
4. Configure the first highlighted task to run **BUSY (75%)**.

13.6.12 Task 5: Verify the results

- Switch to **SEA-CL1**, and then open **Forwarded Events**. In **Performance Monitor**, are any performance-related alerts in the subscribed application log? Hint: They have an ID of 2031.

13.7 lab: title: 'Lab: Migrating server workloads' module: 'Module 12: Upgrade and migration in Windows Server'

14 Lab: Migrating server workloads

14.1 Scenario

Contoso, Ltd. is an engineering, manufacturing, and distribution company. The organization is based in London, England, and it has major offices in Toronto, Canada, and Sydney, Australia.

Because Contoso has been in business for many years, the existing servers include many versions of Windows Server. You're planning to migrate those services to servers running Windows Server 2019.

14.2 Objectives

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

- Select a process to migrate server workloads.
- Plan how to migrate files with Storage Migration Service.

14.3 Estimated time: 20 minutes

14.4 Lab setup

This lab doesn't require virtual machines (VMs).

14.5 Exercise 1: Selecting a process to migrate server workloads

14.5.1 Scenario

Contoso has an Active Directory Domain Services (AD DS) forest with a single Active Directory domain named `contoso.com`. The domain controllers for the domain are running a mix of Windows Server 2012 R2 and Windows Server 2016. Many applications are installed in the domain; standardizing on using Windows Server 2019 for all domain controllers is the best option for you.

Trey Research, a specialist engineering company, has been purchased by Contoso. Trey has its own AD DS forest connected by a forest trust. Much of the Trey infrastructure is old, so you need to standardize tools and management systems across the two companies.

There are other server workloads on servers running earlier versions of Windows Server. For example, the Toronto location has Dynamic Host Configuration Protocol (DHCP) on a server running Windows Server 2012 R2. You want to migrate as many of these server workloads as possible to Windows Server 2019.

The main tasks for this exercise are to:

1. Study the scenario.
2. Plan how to update domains controllers to Windows Server 2019.
3. Plan how to migrate other server workloads.

14.5.2 Task 1: Study the scenario

1. Study the lab scenario.
2. Study the exercise scenario.

14.5.3 Task 2: Plan how to update domain controllers to Windows Server 2019

Answer the following questions based on the scenario:

1. To implement domain controllers running Windows Server 2019, should you upgrade the existing AD DS forest or migrate to a new AD DS forest?
2. What are the highest domain and forest functional levels that you can implement?
3. Which domain controller operating systems can you use to implement the highest possible domain and forest functional levels?
4. What steps do you need to take before adding domain controllers running Windows Server 2019 to an existing AD DS forest?

5. What do you need to consider when removing domain controllers running previous Windows Server versions?

14.5.4 Task 3: Plan how to migrate other server workloads

Answer the following questions based on the scenario:

1. What steps do you need to perform before running the Windows PowerShell cmdlets in the Windows Server Migration Tools on Windows Server 2019?
2. What steps do you need to perform on a source server running Windows Server 2012 R2 before you can use the Windows PowerShell cmdlets in the Windows Server Migration Tools?
3. Which cmdlet can you use to verify which features can be migrated from a source server?
4. List the high-level steps for using the Windows Server Migration Tools to migrate settings from a source server to a destination server.

14.6 Exercise 2: Planning how to migrate files by using Storage Migration Service

14.6.1 Scenario

Contoso has file servers running multiple versions of Windows Server. The oldest file server is running Windows Server 2003. There are also a few Linux servers being used for file storage by developers. Some of the Linux servers are using Samba, but others are using Network File System (NFS). A new policy is being implemented that requires all file servers to be migrated to Windows Server 2019.

The main tasks for this exercise are to:

1. Study the scenario.
2. Plan the migration of file servers.
3. Plan how to use Storage Migration Service.

14.6.2 Task 1: Study the scenario

1. Study the lab scenario.
2. Study the exercise scenario.

14.6.3 Task 2: Plan the migration of file servers

Answer the following questions based on the scenario:

1. Can you use Storage Migration Service to migrate file shares from Windows Server 2003 to Windows Server 2019?
2. Can you use Storage Migration Service to migrate files on Linux servers?
3. Can you use Storage Migration Service to combine multiple file servers to a single new server?
4. Can you use Storage Migration Service to migrate file shares to a VM in Azure?

14.6.4 Task 3: Plan how to use Storage Migration Service

Answer the following questions based on the scenario:

1. What software do you need to install to use Storage Migration Service?
2. What firewall configuration do you need to implement to use Storage Migration Service?
3. What accounts and permissions must be configured to use Storage Migration Service?
4. Which tool do you use to create and manage jobs?
5. What is the relationship between volumes in the source server and the destination server?
6. After cutover, which identity information is moved from the source server to the destination server?
7. Which data won't be migrated from the source server to the destination server?

14.7 lab: title: 'Lab: Deploying and configuring Windows Server' type: 'Answer Key' module: 'Module 1: Windows Server administration'

15 Lab: Deploying and configuring Windows Server

15.1 Scenario

Contoso, Ltd. wants to implement several new servers in their environment, and they have decided to use Server Core. They also want to implement Windows Admin Center for remote management of both these servers and other servers in the organization.

15.2 Objectives

- Deploy and configure Server Core
- Implement and configure Windows Admin Center

15.3 Estimated time: 45 minutes

15.4 Lab setup

VMs: **WS-011T00A-SEA-DC1-B**, **WS-011T00A-SEA-ADM1-B**, **WS-011T00A-SEA-SVR4**

Username: **Contoso\Administrator**

Password: **Pa55w.rd**

For this lab, you'll use the available VM environment. Before you begin the lab, complete the following steps:

1. Start **WS-011T00A-SEA-DC1-B**.
2. Start **WS-011T00A-SEA-ADM1-B**.

15.5 Exercise 1: Deploying and configuring Server Core

15.5.1 Scenario

As a part of the deployment plan, you will implement Server Core and configure it for remote management. **WS-011T00A-SEA-SVR4-B** is pre-configured to turn on from the **Win2019_1809_Eval.iso** to install Windows Server.

The main tasks for this exercise are as follows:

1. Install Server Core.
2. Configure Server Core with sconfig and PowerShell.
3. Install Features on Demand on Server Core.

15.5.2 Task 1: Install Server Core

1. Start **WS-011T00A-SEA-SVR4-B**. Windows will start loading the installation files.
2. At the **Windows Setup** page, note the **Language, Time and Keyboard** settings, and then select **Next**.
3. Select **Install now**.
4. On the **Select the operating system you want to install** page, ensure that **Windows Server 2019 Standard Evaluation** is selected, and then select **Next**.
5. Select the **I accept license terms** check box to accept the license terms, and then select **Next**.
6. On the **Which type of installation do you want?** page, select **Custom: Install Windows only (advanced)**.
7. On the **Where do you want to install Windows?** page, select **Next**. Installation will take a few minutes.
8. After installation completes, select Ctrl-Alt-Del. After reading the message about changing the password, select Enter.
9. In the **New password** and **Confirm password** fields, enter **Pa55w.rd**, and then select Enter twice to acknowledge the password has been changed.

15.5.3 Task 2: Configure Server Core with sconfig and PowerShell

1. At the command prompt, enter **sconfig**, and then select Enter.
2. To access **Network Settings**, enter **8**, and then select Enter.
3. To change adapter index #1, enter **1**, and then select Enter.
4. To set the network adapter address, enter **1**, and then select Enter.
5. To set a static IP address, enter **S**, and then select Enter.
6. To set the IP address, enter **172.16.10.15**, and then select Enter.
7. To set the subnet mask, enter **255.255.0.0**, and then select Enter.
8. To set the Default Gateway and observe the resulting settings, enter **172.16.10.1**, and then select Enter.
9. To set the Domain Name System (DNS) server, enter **2**, and then select Enter.
10. Enter **172.16.10.10**, and then select Enter. Then, to dismiss the message box, select **OK**. To leave the alternate DNS server blank, select Enter.
11. To return to the main menu, enter **4**, and then select Enter.
12. To exit to Command Line, enter **15**, and then select Enter.
13. At the command prompt, enter **PowerShell**, and then select Enter.
14. At the PowerShell prompt, enter `Rename-Computer -NewName SEA-SVR4 -restart -force`, and then select Enter.
15. On **SEA-SVR4**, select Ctrl+Alt+Del, enter the password **Pa55w.rd**, and then select Enter.
16. At the command prompt, enter **PowerShell**, and then select Enter.
17. At the PowerShell prompt, enter `Add-Computer -DomainName Contoso.com -Credential Contoso\Administrator -restart -force`, and then select Enter. In the **Windows PowerShell credential request** window, enter **Pa55w.rd**, and then select **OK**.

15.5.4 Task 3: Install Features on Demand on Server Core

1. Mount the **Win2019_FOD.iso** image file to drive D of SEA-SVR4.
2. On SEA-SVR4, select Ctrl+Alt+Del, enter the password **Pa55w.rd**, and then select Enter.
3. At the command prompt, enter **Explorer.exe**. Note that the command does not run and returns an error.
4. At the command prompt, enter **PowerShell**, and then select Enter.
5. At the PowerShell prompt, enter `Add-Windowscapability -Online -Name Servercore.Appcompatibility~~~~0.0.1 -Source D:`.
6. After completion, to restart the server and then sign in with the password **Pa55w.rd** at the PowerShell prompt, enter **Restart-computer**.
7. At the command prompt, enter **Explorer.exe**. Note that File Explorer now opens successfully.

15.5.5 Results

After completing this exercise, you will have installed Server Core, configured the networking settings, renamed the server, and joined the Contoso domain.

15.6 Exercise 2: Implementing and using remote server administration

15.6.1 Scenario

Now that you have deployed the Server Core servers, you need to implement Windows Admin Center for remote administration.

The main tasks for this exercise are as follows:

1. Install Windows Admin Center.
2. Add servers for remote administration.
3. Configure Windows Admin Center extensions.
4. Verify remote administration.
5. Administer servers with Remote PowerShell.

15.6.2 Task 1: Install Windows Admin Center

1. Connect to **WS-011T00A-SEA-ADM1-B**.
2. Select Ctrl+Alt+Del and sign in as **Contoso\Administrator** with a password of **Pa55w.rd**.
3. From the taskbar, open File Explorer, and then browse to **C:\Labfiles\Mod01**.
4. Double-click or select **WindowsAdminCenter1910.2.msi**.

5. On the **Windows Admin Center Setup** page, to accept the terms, select the check box, and then select **Next**.
6. On the **Use Microsoft Update to help keep your computer secure and up-to-date** page, select **Next**.
7. On the **Install Windows Admin Center on Windows Server** page, select **Next**.
8. On the **Configure Gateway Endpoint** page, select **Next**, and then select **Install**.
9. Select **Finish**.

15.6.3 Task 2: Add servers for remote administration

1. From the taskbar, open Microsoft Edge.
2. In the address bar, enter `Https://Sea-Adm1`, and then select Enter. The console will open. Notice that the host server is listed by default.
3. In Windows Admin Center, select **Add**.
4. In the Add resources pane, in the Windows Server box, select **Add**
5. In the **Server name** box, enter **SEA-DC1**. In a few moments, the server will be found through DNS, and then select **Add**. .
6. Select **Add**.
7. Repeat the steps to add **SEA-SVR4**.

15.6.4 Task 3: Configure Windows Admin Center extensions

1. In the upper right corner, select the **Settings** icon (the cog wheel).
2. In the left pane, select **Extensions**. Note that there are no available extensions.
3. In the **details** pane, select **Feeds**, and then select **Add**.
4. In the **Add package source** pane, in the **Extension feed** URL or path, enter **C:\Labfiles\Mod01**, and then select **Add**.
5. Select **Available extensions**. Now you can observe the extensions.
6. Select the **DNS (Preview)** extension, and then select **Install**. The extension will install and Windows Admin Center will refresh.
7. On the top menu, next to **Settings**, select the drop-down arrow, and then select **Server Manager**.
8. On the **Server connections** page, select the `SEA-DC1.Contoso.com` link.
9. To install the DNS PowerShell tools in the left pane, select **DNS**, and then select **Install**. The tools will take a few moments to install.
10. Select the `Contoso.com` zone and observe the console.

15.6.5 Task 4: Verify remote administration

1. In Windows Admin Center, select the **Overview** icon in the left pane. Note that the **details** pane for Windows Admin Centers displays basic server information and performance monitoring, which is like **Task Manager**.
2. In the left pane, scroll down and observe the basic administration tools available. Select **Roles and Features** and note what is installed and what is available to install. Scroll down and check the box beside **Telnet Client**, and then select **Install**, which will be at the top of the list.
3. To install the Telnet Client, select **Yes**. In a few moments, you will get a message that the Telnet Client installed successfully.
4. In the **details** pane, select **Remote Desktop**, select **Go to settings**, select the **Allow remote connections to this computer** radio button, and then select **Save**.
5. Close the browser.

15.6.6 Task 5: Administer servers with Remote PowerShell

1. Select **Start**, enter **PowerShell**, and then select Enter.
2. At the PowerShell prompt, enter `Enter-PSSession -ComputerName SEA-DC1`, and then select Enter.
3. Enter `Get-Service -Name AppIDSvc`, and then select Enter. Note that the service is currently stopped.
4. Enter `Start-Service -Name AppIDSvc`, and then select Enter.
5. Enter `Get-Service -Name AppIDSvc`, and then select Enter. Note that the service is currently running.

15.6.7 Results

15.7 After completing this exercise, you will have installed Windows Admin Center and connected the server to manage. You performed management tasks of installing a feature and enabling Remote Desktop. Finally, you used Remote PowerShell to check the status of a service and start a service.

15.8 lab: title: 'Lab: Implementing identity services and Group Policy' type: 'Answer Key' module: 'Module 2: Identity services in Windows Server'

16 Lab answer key: Implementing identity services and Group Policy

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

16.1.1 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:

   ```
   Install-WindowsFeature -Name AD-Domain-Services -ComputerName SEA-SVR1
   ```

4. Enter the following command to verify that the AD DS role is installed on **SEA-SVR1**, and then select Enter:

   ```
   Get-WindowsFeature -ComputerName SEA-SVR1
   ```

5. 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.

6. On **SEA-ADM1**, in **Server Manager**, select the **All Servers** view.
7. On the **Manage** menu, select **Add Servers**.
8. In the **Add Servers** dialog box, maintain the default settings, and then select **Find Now**.
9. In the **Active Directory** list of servers, select **SEA-SVR1**, select the arrow to add it to the **Selected** list, and then select **OK**.
10. 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.
11. Note the post-deployment configuration of **SEA-SVR1**, and then select the **Promote this server to a domain controller** link.
12. 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.
13. Ensure that the `Contoso.com` domain is specified, and then in the **Supply the credentials to perform this operation** section, select **Change**.
14. In the **Credentials for deployment operation** dialog box, in the **User name** box, enter **Contoso\Administrator**, and then in the **Password** box, enter **Pa55w.rd**.

15. Select **OK**, and then select **Next**.
16. 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.
17. In the **Type the Directory Services Restore Mode (DSRM) password** section, enter and confirm the password **Pa55w.rd**, and then select **Next**.
18. On the **DNS Options** page, select **Next**.
19. On the **Additional Options** page, select **Next**.
20. On the **Paths** page, keep the default path settings for the **Database** folder, **Log files** folder, and **SYSVOL** folder, and then select **Next**.
21. On the **Review Options** page, select **View script** to open the generated Windows PowerShell script.
22. 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.
23. 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**.
24. Switch to the **Active Directory Domain Services Configuration Wizard**, and then select **Cancel**.
25. When prompted for confirmation, select **Yes** to cancel the wizard.
26. At the Windows PowerShell command prompt, enter the following command:

    ```
    Invoke-Command -ComputerName SEA-SVR1 { }
    ```

27. 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:

    ```
    Invoke-Command -ComputerName SEA-SVR1 {Install-ADDSDomainController -NoGlobalCatalog:\$false -Crea
    ```

28. Select Enter to start the command.
29. In the **Windows PowerShell Credential Request** dialog box, enter **Contoso\Administrator** in the **User name** box, enter **Pa55w.rd** in the **Password** box, and then select **OK**.
30. When prompted for the password, in the **SafeModeAdministratorPassword** text box, enter **Pa55w.rd**, and then select Enter.
31. When prompted for confirmation, in the **Confirm SafeModeAdministratorPassword** text box, enter **Pa55w.rd**, and then select Enter.
32. Wait until the command runs and the **Status Success** message is returned. The **SEA-SVR1** virtual machine restarts.
33. Close Notepad without saving the file.
34. 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**.

16.2 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:

    ```
    New-ADOrganizationalUnit -Name:"Seattle" -Path:"DC=Contoso,DC=com" -ProtectedFromAccidentalDeletio
    ```

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

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

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

   ```
   Set-ADAccountPassword Ty
   ```

6. When you receive a prompt for the current password, select Enter.
7. When you receive a prompt for the desired password, enter **Pa55w.rd**, and then select Enter.
8. When you receive a prompt to repeat the password, enter **Pa55w.rd**, and then select Enter.
9. To enable the account, run the following command:

   ```
   Enable-ADAccount Ty
   ```

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

    ```
    New-ADGroup SeattleBranchUsers -Path "ou=Seattle,dc=contoso,dc=com" -GroupScope Global -GroupCateg
    ```

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

    ```
    Add-ADGroupMember SeattleBranchUsers -Members Ty
    ```

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

    ```
    Get-ADGroupMember SeattleBranchUsers
    ```

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

16.3 Exercise 2: Configuring Group Policy

16.3.1 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.

16.3.2 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**.

16.3.3 Task 3: Review the effects of the GPO's settings

1. Switch to **SEA-CL1**, and then sign in as **Contoso\Administrator** 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\Ty** 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.
11. Right-click or access the context menu for **Start**, and then select **Run**.
12. In the **Run** dialog box, in the **Open** text box, enter **regedit**, and then select **OK**.
13. In the **Registry Editor** dialog box, select **OK**.

16.3.4 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.

16.3.5 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.

16.3.6 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 Contoso\Ty on SEA-CL1 before preceding with the next step.

16.3.7 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\Ty**, 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.

16.4 Exercise 3: Deploying and using certificate services

16.4.1 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.

16.4.2 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**.

16.4.3 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
   ```

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

2. From **Server Manager**, select **Tools**, and then select **Internet Information Services (IIS) Manager**.
3. Select **SEA-ADM1**, and then in the central pane, double-click **Server Certificates** or select it and then select Enter.
4. In the **Actions** pane, select **Create Domain Certificate**.
5. 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**
6. On the **Online Certification Authority** page, select **Select**, select **ContosoCA**, and then select **OK**.
7. In the **Friendly name** text box, enter **sea-adm1**, and then select **Finish**.
8. Ensure that the certificate displays in the **Server Certificates** console.
9. In the **IIS** console, expand **SEA-ADM1**, expand **Sites**, and then select **Default Web Site**.
10. In the **Actions** pane, select **Bindings**.
11. In the **Site Bindings** window, select **Add**.
12. 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**.
13. 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?

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

16.6 lab: title: 'Lab: Implementing and configuring network infrastructure services in Windows Server' type: 'Answer Key' module: 'Module 3: Network Infrastructure services in Windows Server'

17 Lab answer key: Implementing and configuring network infrastructure services in Windows Server

17.1 Exercise 1: Deploying and configuring DHCP

17.1.1 Task 1: Install the DHCP role

1. On **SEA-ADM1**, on the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, select **Windows Admin Center**.

3. In the **Windows Security** dialog box, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
4. In **Windows Admin Center**, select **SEA-SVR1**.
5. In the **Specify your credentials** dialog box, select **Use another account** for this connection, and then sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
6. On the **Tools** pane, select **Roles & features**.
7. In the **Roles and features** pane, select the **DHCP Server** check box, and then select **Install**.
8. In the **Install Roles and Feature**s dialog box, select **Yes**.
9. Wait until a notification displays indicating that the DHCP role is installed. If necessary, select the **Notifications** icon to verify the current status.
10. In **Microsoft Edge**, select **Windows Admin Center**, and then select **SEA-SVR1**.
11. On the **Tools** pane, select **DHCP**, and then on the **details** pane, select **Install**. If DHCP is not available in the **Tools** pane for **SEA-SVR1**, close **Microsoft Edge** and sign in to **Windows Admin Center** again.
12. Wait for a notification that the DHCP PowerShell tools are installed. If necessary, select the **Notifications** icon to verify the current status.

17.1.2 Task 2: Authorize the DHCP server

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Notifications** in the menu, and then select **Complete DHCP configuration**.
3. In the **DHCP Post-Install configuration wizard** window, on the **Description** screen, select **Next**.
4. On the **Authorization** screen, select **Commit** to use the **Contoso\Administrator** credentials.
5. When you complete both tasks, select **Close**.

17.1.3 Task 3: Create a scope

1. On **SEA-ADM1**, in **Windows Admin Center**, while connected to **SEA-SVR1**, in the **Tools** pane, select **DHCP**, and then select **New scope**.
2. In the **Create a new scope** dialog box, enter the following information, and then select **Create**.
   - Protocol: **IPv4**
   - Name: **ContosoClients**
   - Starting IP address: **10.100.150.50**
   - Ending IP address: **10.100.150.254**
   - DHCP client subnet mask: **255.255.255.0**
   - Router: **10.100.150.1**
   - Lease duration: **4 days**
3. In **Server Manager**, select **Tools**, and then select **DHCP**.
4. In the DHCP window, select **Action**, and then select **Add Server**.
5. In the **Add Server** dialog box, select **This authorized DHCP server**, and then select **OK**.
6. In DHCP window, expand **172.16.10.12**, expand **IPv4**, expand **Scope [10.100.150.0] ContosoClients**, and then select **Scope Options**.
7. Select the **Action** menu, and then select **Configure Options**.
8. In the **Scope Options** dialog box, select the **006 DNS Servers** check box.
9. In the IP address box, enter **172.16.10.10**, select **Add**, and then select **OK**.

17.1.4 Task 4: Configure DHCP Failover

1. On **SEA-ADM1**, in the DHCP window, select **IPv4**, select the **Action** menu, and then select **Configure Failover**.
2. In the **Configure Failover** window, verify that the **Select all** check box is checked, and then select **Next**.
3. On the **Specify the partner server to use for failover** screen, in the **Partner Server** box, enter **SEA-DC1**, and then select **Next**.
4. On the **Create a new failover relationship** screen, enter the following information, and then select **Next**.
   - Relationship Name: **SEA-SVR1 to SEA-DC1**
   - Maximum Client Lead Time: **1 hour**
   - Mode: **Hot standby**
   - Role of Partner Server: **Standby**
   - Addresses reserved for standby server: **5%**

- State Switchover Interval: **Disabled**
- Enable Message Authentication: **Enabled**
- Shared Secret: **DHCP-Failover**

5. Select **Finish**.
6. In the **Configure Failover** dialog box, select **Close**.
7. Under **172.16.10.12**, select **IPv4**, and then verify that only one scope is listed.
8. Expand **SEA-DC1**, select **IPv4**, and then verify that two scopes are listed.
9. Select **Scope [172.16.0.0] Contoso**, select the **Action** menu, and then select **Configure Failover**.
10. In the **Configure Failover** window, select **Next**.
11. On the **Specify the partner server to use for failover** screen, in the **Partner Server** box, enter **172.16.10.12**, select the **Reuse existing failover relationships configured with this server (if any exist)** check box, and then select **Next**.
12. On the **Select from failover relationships which are already configured on this server** screen, select **Next**, and then select **Finish**.
13. In the **Configure Failover** dialog box, select **Close**.
14. Under **172.16.10.12**, select **IPv4**, and then verify that both scopes are listed. If necessary, select **F5** to refresh.

17.1.5 Task 5: Verify DHCP functionality

1. On **SEA-CL1**, select **Start**, and then select **Settings**.
2. In the **Settings** window, select **Network & Internet**, and then select **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Ethernet**, and then select **Properties**.
4. In the **Ethernet Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.
5. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Obtain an IP address automatically**, select **Obtain DNS server address automatically**, and then select **OK**.
6. Select **Close**, and then select **Details**.
7. In the **Network Connection Details** dialog box, verify that DHCP is enabled, an IP address was obtained, and that the **SEA-SVR2 (172.16.10.12)** DHCP server issued the lease.
8. Select **Close**, and then select **Disable**.
9. On **SEA-ADM1**, in the **DHCP** window, under **172.16.10.12**, under **IPv4**, expand **Scope [172.16.0.0] Contoso**, and then select **Address Leases**.
10. 1. Verify that **SEA-CL1** is listed as a lease.
11. Under **SEA-DC1**, under **IPv4**, expand **Scope [172.16.0.0] Contoso**, and then select **Address Leases**.
12. Verify that **SEA-CL1** is listed as a lease.
13. Select **172.16.10.12**, select the **Action** menu, select **All Tasks**, and then select **Stop**.
14. Close all open windows on **SEA-ADM1**.
15. On **SEA-CL1**, in the **Network and Sharing Center**, on the left **navigation** pane, select **Change adapter settings**.
16. In the **Network Connections** window, right-click or access the context menu for **Ethernet**, and then select **Enable**.
17. In the menu bar, select **View status of this connection**, and then select **Details**. Verify that the DHCP server is now **SEA-DC1 (172.16.10.10)**.
18. Close all open windows on **SEA-CL1**.

17.2 Exercise 2: Deploying and configuring DNS

17.2.1 Task 1: Install the DNS role

1. On **SEA-ADM1**, On the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, select **Windows Admin Center**.

3. In the **Windows Security** dialog box, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
4. In **Windows Admin Center**, select **SEA-SVR1**.
5. In the **Specify your credentials** dialog box, select **Use another account for this connection**, and then sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
6. In the **Tools** pane, select **Roles & features**.
7. In the **Roles and features** pane, select the **DNS Server** check box, and then select **Install**.
8. In the **Install Roles and Features** dialog box, select **Yes**.
9. Wait until a notification appears indicating that the DNS role is installed. If necessary, select the **Notifications** icon to verify the current status.
10. In **Microsoft Edge**, select **Windows Admin Center**, and then select **SEA-SVR1**.
11. In the **Tools** pane, select **DNS**, and then on the **details** pane, select **Install**. If DNS is not available in the **Tools** pane for **SEA-SVR1**, close **Microsoft Edge** and sign in to **Windows Admin Center** again.
12. Wait until a notification appears indicating that the DNS PowerShell tools are installed. If necessary, select the **Notifications** icon to verify the current status.

17.2.2 Task 2: Create a DNS zone

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Create a new DNS zone**.
2. In the **Create a new DNS zone** dialog box, enter the following information, and then select **Create**:
   - Zone type: **Primary**
   - Zone name: `TreyResearch.net`
   - Zone file: **Create a new file**
   - Zone file name: `TreyResearch.net.dns`
   - Dynamic update: **Do not allow dynamic update**
3. Select `TreyResearch.net`, and then select **Create a new DNS record**.
4. In the **Create a new DNS record** dialog box, enter the following information, and then select **Create**:
   - DNS record type: **Host (A)**
   - Record name: **TestApp**
   - IP address: **172.30.99.234**
   - Time to live: **600**
5. Select **Start**, and then select **Windows PowerShell**.
6. At the **Windows PowerShell** prompt, enter the following, and then select Enter:

   ```
   Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net
   ```

7. Close the **Windows PowerShell** prompt.

17.2.3 Task 3: Configure forwarding

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Tools**, and then select **DNS**.
3. In **DNS Manager**, select **DNS**, select **Action**, and then select **Connect to DNS Server**.
4. In the **Connect to DNS Server** dialog box, select **The following computer**, enter **SEA-SVR1**, and then select **OK**.
5. In **DNS Manager**, select **SEA-SVR1**, select **Action**, and then select **Properties**.
6. In the **SEA-SVR1 Properties** dialog box, select the **Forwarders** tab, and then select **Edit**.
7. In the **Edit Forwarders** dialog box, in the **IP addresses for forwarding servers** box, enter **131.107.0.100**, and then select **OK**.
8. In the **SEA-SVR1 Properties** dialog box, select **OK**.

17.2.4 Task 4: Configure conditional forwarding

1. On **SEA-ADM1**, in **DNS Manager**, expand **SEA-SVR1**, and then select **Conditional Forwarders**.
2. Select **Action**, and then select **New Conditional Forwarder**.
3. In the **New Conditional Forwarder** dialog box, in the **DNS Domain** box, enter `Contoso.com`.
4. In the **IP addresses of the master servers** box, enter **172.16.10.10**, and then select **Enter**.

5. Select **OK**.
6. Close **DNS Manager** and **Server Manager**.
7. Select **Start**, and then select **Windows PowerShell**.
8. At the **Windows PowerShell** prompt, enter the following, and then select Enter:

   ```
   Resolve-DnsName -Server sea-svr1.contoso.com -Name sea-dc1.contoso.com
   ```

9. Close the Windows PowerShell prompt.

17.2.5 Task 5: Configure DNS policies

1. On **SEA-ADM1**, in Windows Admin Center, while connected to **SEA-SVR1**, use PowerShell to sign in remotely.
2. At the **Password** prompt, enter **Pa55w.rd**, and then select **Enter**.
3. To create a head office subnet, enter the following, and then select Enter:

   ```
   Add-DnsServerClientSubnet -Name "HeadOfficeSubnet" -IPv4Subnet "172.16.10.0/24"
   ```

4. To create a zone scope for head office, enter the following, and then select Enter:

   ```
   Add-DnsServerZoneScope -ZoneName "TreyResearch.net" -Name "HeadOfficeScope"
   ```

5. To add a new resource record for the head office scope, enter the following, and then select Enter:

   ```
   Add-DnsServerResourceRecord -ZoneName "TreyResearch.net" -A -Name "testapp" -IPv4Address "172.30.9
   ```

6. To create a new policy that links the head office subnet and the zone scope, enter the following, and then select Enter:

   ```
   Add-DnsServerQueryResolutionPolicy -Name "HeadOfficePolicy" -Action ALLOW -ClientSubnet "eq,HeadO
   ```

7. Close **Windows Admin Center**.

17.2.6 Task 6: Verify DNS policy functionality

1. On **SEA-CL1**, right-click or access the context menu for **Start**, and then select **Windows PowerShell**.
2. At the **Windows PowerShell** prompt, enter **ipconfig**, and then select **Enter**. Note that the Ethernet adapter has an IP address that is part of the HeadOfficeSubnet configured in the policy.
3. Enter `Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net`, and then select **Enter**. The name resolves to the IP address 172.30.99.100 that was configured in the HeadOfficePolicy.
4. Select **Start**, and then select **Settings**.
5. In the **Settings** window, select **Network & Internet**, and then select **Network and Sharing Center**.
6. In **Network and Sharing Center**, select **Ethernet**, and then select **Properties**.
7. In the **Ethernet Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.
8. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Use the following IP address**, enter the following information, and then select **OK**:
   - IP Address: **172.16.11.100**
   - Subnet mask: **255.255.0.0**
   - Default gateway: **172.16.10.1**
   - Preferred DNS server: **172.16.10.10**
9. Select **Close** twice.
10. At the **Windows PowerShell** prompt, enter the following, and then select Enter:

    ```
    Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net
    ```

11. Notice that the name resolves to **172.30.99.234** because the client is no longer on the HeadOffice subnet.
12. Close all open windows.

Note: When the client is on the HeadOffice subnet **(172.16.10.0/24)** the record testapp.`treyresearch.net` resolves to **172.30.99.100**. When the client is moved off of the HeadOffice subnet, `testapp.treyresearch.net` resolves to **172.30.99.234**.

17.3 lab: title: 'Lab: Implementing storage solutions in Windows Server' type: 'Answer Key' module: 'Module 4: File servers and storage management in Windows Server'

18 Lab answer key: Implementing storage solutions in Windows Server

Note: Be sure to revert the virtual machines (VMs) between each exercise. Due to most of the VMs being Windows Server 2019 Server Core, the time it takes to revert and restart is faster than attempting to undo changes made to the storage environment in the exercises.

18.1 Exercise 1: Implementing Data Deduplication

18.1.1 Task 1: Install the Data Deduplication role service

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In Server Manager, select **Manage**, and then select **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, select **Next** twice.
4. On the **Select destination server** page , in the **Server Pool** pane, select `SEA-SVR3.Contoso.com`, and then select **Next**.
5. On the **Select server roles** page, in the **Roles** pane, expand the **File and Storage Services** item, and then expand the **File and iSCSI Services** item, select the **Data Deduplication** item, and then select **Next**.
6. On the **Select features** page, select **Next**, and then in the **Confirm installation selections** page, select **Install**.
7. While the role service is installing, on the taskbar, select the **File Explorer** icon.
8. In **File Explorer**, expand drive **C**.
9. Right-click or access the context menu for the **Labfiles** directory, and then select **Give access to**. In the next context menu, select **Specific people...**.
10. In the **Type a name and then Click Add, or click the arrow to find someone** text box, type **Users** and click **Add**.
11. In the **Network access** window, select **Share**, and when the **Your folder is shared** section opens, select **Done**.
12. 2. In Server Manager, on the **Add Roles and Features Wizard installation succeeded** page, select **Close**.
13. Switch to **SEA-SVR3**.
14. In the **Command Prompt** window, enter **PowerShell**.
15. Note that the prompt changes with the **PS** cursor to let you know you are now in Windows PowerShell.
16. In the **Administrator: Windows PowerShell** window, enter the following commands, selecting Enter after each line.

```
Get-Disk

Initialize-Disk -Number 1

New-Partition -DiskNumber 1 -UseMaximumSize -DriveLetter M

Format-Volume -DriveLetter M -FileSystem ReFS

Exit
```

17. In the **Command Prompt** window, enter the following command, selecting Enter after each line:

    ```
    Net use x: \\SEA-ADM1\Labfiles

    M:

    Md Data

    copy x:\mod04\createlabfiles.cmd M:

    CreateLabFiles.cmd

    Cd data

    dir
    ```

18. Make note of the free space in **M:\Data**.

18.1.2 Task 2: Enable and configure Data Deduplication

1. Return to **SEA-ADM1**
2. In the Server Manager console tree, right-click or access the context menu for **File and Storage Services**, and then from the context menu select **Disks**
3. In the **Disks** pane, select **SEA-SVR3**, **Number** column **1**.
4. In the **Volumes** pane, right-click or access the context menu for the **M** volume, and then from the context menu, select **Configure Data Deduplication**.
5. In the **Volume (M:) Deduplication Settings** wizard, select the Data Deduplication drop-down menu and change the selection to the **General purpose file server** setting.
6. Set **Deduplicate files older than (in days):** to **0**.
7. Select the **Set Deduplication Schedule** button.
8. In the **SEA-SVR3 Deduplication Schedule** window, select **Enable throughput optimization**, and then select **OK**.
9. In the **Volume (M:) Deduplication Settings Wizard**, select **OK**.

18.1.3 Task 3: Test Data Deduplication

1. On **SEA-ADM1**, on the taskbar, select **Microsoft Edge**.
2. In Microsoft Edge, select the **Windows Admin Center** (WAC) tab on the **Favorites** bar.
3. In the **Windows Security** pop-up window, in the **User name** text box, enter **Contoso\Administrator**, in the **Password** text box, enter **Pa55w.rd**, and then select **OK**.
4. On the **All connections** page, select **SEA-SVR3**.
5. On the **Specify your credentials** blade, select the **Use another account for this connection** radio button.
6. In the **Username** text box, enter **Contoso\Administrator**, and in the **Password** text box, enter **Pa55w.rd**, select the check box for **Use these credentials for all connections**, and then select **Continue**.
7. In the **SEA-SVR3 Tools** console, scroll to and select the **PowerShell** node.
8. In the **PowerShell** pane, enter **Pa55w.rd** at the **Password** prompt.
9. In the **PowerShell** pane, enter the following command, and then select Enter:

    ```
    Start-DedupJob m: -Type Optimization -Memory 50
    ```

10. Switch to **SEA-SVR3**.
11. In the **Command Prompt** window, enter **Dir**.
12. Observe the **Bytes free** size on property values for the **Data** Directory.
13. Wait for five to ten minutes to allow the deduplication job to run.
14. Repeat step 12.
15. Switch back to **SEA-ADM1**, and to the **WAC SEA-SVR3 PowerShell** pane.

16. To verify the Data Deduplication status, run the following commands, pressing Enter at the end of each line:

    ```
    Get-DedupStatus -Volume M: | fl
    ```

    ```
    Get-DedupVolume -Volume M: |fl
    ```

    ```
    Get-DedupMetadata -Volume M: |fl
    ```

17. In **Server Manager**, select **File and Storage Services**, select disk **1**, and then select Volume **M**.
18. Observe the values for **Deduplication Rate** and **Deduplication Savings**.

    Note: When you have finished the exercise, revert the VMs to their initial state.

18.2 Exercise 2: Configuring iSCSI storage

18.2.1 Task 1: Install iSCSI and configure targets

1. On **SEA-ADM1**, right-click or access the context menu for **Start**, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    Invoke-Command -ComputerName SEA-SVR3 -ScriptBlock {Install-WindowsFeature -Name FS-iSCSITarget-Se
    IncludeManagementTools}
    ```

3. Enter the following command, and then select Enter:

    ```
    Enter-PSSession -ComputerName SEA-SVR3 -Credential "Contoso\Administrator"
    ```

4. In the **Windows PowerShell credential request** pop-up window, in the **Password** text box, enter **Pa55w.rd**, and then select **OK**.
5. In the **Administrator: Windows PowerShell** window, enter the following commands, pressing Enter at the end of each line:

    > **Note**: In the following command, drive Y is placeholder text only. The drive letter to use will be returned to you in the results of the second command.

    ```
    Initialize-Disk -Number 2
    New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter
    Format-Volume -DriveLetter _Y_ -FileSystem ReFS
    ```

6. Repeat step 5 for disk 3, replacing 2 with the number 3.
7. In the **Administrator: Windows PowerShell** window, enter the following commands, pressing Enter at the end of each line:

    ```
    New-NetFirewallRule -DisplayName "iSCSITargetIn" -Profile "Any" -Direction Inbound -Action Allow -
    ```

    ```
    New-NetFirewallRule -DisplayName "iSCSITargetOut" -Profile "Any" -Direction Outbound -Action Allow
    ```

8. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    Exit-PSSEssion
    ```

18.2.2 Task 2: Connect to and configure iSCSI targets

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In Server Manager, in the console tree, select **File and Storage Services**, and then under **Disks** pane, select the **SEA-DC1** server. Note that the server only contains the boot and system volume drive C.
3. In the same pane, select the **SEA-SVR3** server. Note that disks **2**, **3**, and **4** are still offline.
4. Right-click or access the context menu for each disk, and in the context menu, select **Bring online**.
5. In the **Bring Disk Online** window, select **Yes**.
6. In the **Server Manager** window, in **File and Storage Services**, select **iSCSI**, select **Tasks**, and in the context menu, select **New iSCSI Virtual Disk**.

7. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under the **SEA-SVR3** server, select the **E:** volume, and then select **Next**.
8. In the Specify iSCSI virtual disk name page, in the **Name** text box, enter **iSCSIDisk1**, and then select **Next**.
9. On the **Specify iSCSI virtual disk size** page, in the **Size** text box, enter **5**. Leave all other settings as they are, and then select **Next**.
10. On the **Assign iSCSI target** page, ensure the **New iSCSI target** radio button is selected, and then select **Next**.
11. In the **Specify target name** page, in the **Name** field, enter **iSCSIFarm**, and then select **Next**.
12. In the **Specify access servers** page, select the **Add** button.
13. In the **Select a method to identify the initiator** window, select the **Browse** button.
14. In the **Select Computer** window, in the **Enter the object name to select** text box, enter **SEA-DC1**, select **Check Names**, and then select **OK**.
15. In the **Select a method to identify the initiator** window, select **OK**.
16. On the **Specify access servers** page, select **Next**.
17. On the **Enable Authentication** page, select **Next**.
18. On the **Confirm selections** page, select **Create**.
19. On the **View results** page, select **Close**.
20. Create the second iSCSI virtual disk (F:), by repeating steps 4 through 9 and then step 17, using the following settings:
    - Storage Location: **F:**
    - Name: **iSCSIDisk2**
    - Disk size: **5 GB**, **Dynamically Expanding**
    - iSCSI target: **iSCSIFarm**
21. On **SEA-DC1**, in the Command Prompt window, enter **PowerShell.**.
22. In the **Windows PowerShell** window, enter the following commands, selecting **Enter** after each command:

    ```
    Start-Service msiscsi
    ```

    ```
    iscsicpl
    ```

    Note: The **iscsicpl** command will open an **iSCSI Initiator Properties** dialog box.
23. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, in the **Target** text box, enter **SEA-SVR3**, and then select **Quick Connect**.
24. In the **Quick Connect** dialog box, note that the **Discovered target name** is **iqn.1991-05.com.microsoft:sea-svr3-iscscifarm-target**, and then select **Done**.
25. In the **iSCSI Initiator Properties** dialog box, select **OK**.
26. Close the **iSCSI Initiator Properties** dialog box.

18.2.3 Task 3: Verify iSCSI disk presence

1. Switch back to **SEA-ADM1**.
2. In **Server Manager**, select **File and Storage Services**, and then select **Disks**. In the **Tasks** drop-down list box, select **Refresh**.
3. Notice the two new **5 GB** disks on the **SEA-DC1** server that are offline. Notice that the bus entry is **iSCSI**.
4. Switch back to **SEA-DC1**.
5. In the **Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Get-Disk
   ```

Note: Both disks are present and healthy, but offline. To use them, you need to initialize and format them on **SEA-DC1**.

6. In the **Windows PowerShell** window, enter the following commands, selecting Enter after each command:

```
Initialize-Disk -Number 1

New-Partition -DiskNumber 1 -UseMaximumSize -DriveLetter E

Format-Volume -DriveLetter E -FileSystem ReFS
```

7. Repeat step 6 above, using disk number **2** and disk letter **F**.
8. Return to **SEA-ADM1**.
9. In **server Manager**, refresh the page in the **Tasks** drop-down, and note that both the drives are now **Online**.

Note: When you have finished the exercise, revert the VMs to their initial state.

18.3 Exercise 3: Configuring redundant Storage Spaces

18.3.1 Task 1: Create a storage pool by using the iSCSI disks attached to the server

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In Server Manager, in the **navigation** pane, select **File and Storage Services**, and then select **Disks**.
3. In the **Disks** pane, scroll down, and note that the **SEA-SVR3** disks 1 through 4 are set to **Unknown**.
4. Right-click or access the context menu for each offline disk, select **Bring Online**, and then in the **Bring Disk Online** window, select **Yes**.
5. Verify that all disks are now online, and then in Server Manager, in the **navigation** pane, select **File and Storage Services**, and then select **Storage Pools**.
6. In Server Manager, in the **STORAGE POOLS** area, in the **TASKS** list, select **New Storage Pool**.
7. In the **New Storage Pool Wizard**, on the **Before you begin** page, select **Next**.
8. On the **Specify a storage pool name and subsystem** page, in the **Name** text box, enter **SP1**. In the **Description** text box, enter **Storage Pool 1**, and then select **Next**.
9. On the **Select physical disks for the storage pool** page, select the check box for the top three disks, and then select **Next**.
10. On the **Confirm selections** page, review the settings, and then select **Create**.
11. Select **Close**.

18.3.2 Task 2: Create a three-way mirrored disk

1. In **Server Manager**, in **Storage Pools**, select **SP1**.
2. In the **VIRTUAL DISKS** area, select **TASKS**, and then select **New Virtual Disk**.
3. In the **Select the storage pool** dialog box, select **SP1**, and then select **OK**.
4. In the **New Virtual Disk Wizard**, on the **Before you begin** page, select **Next**.
5. On the **Specify the virtual disk name** page, in the **Name** text box, enter **Three-Mirror**,and then select **Next**.
6. On the **Specify enclosure resiliency** page, select **Next**.
7. On the **Select the storage layout** page, select **Mirror**, and then select **Next**.
8. On the **Specify the provisioning enter** page, select **Thin**, and then select **Next**.
9. On the **Specify the size of the virtual disk** page, in the **Specify size** text box, enter **25**, and then select **Next**.
10. On the **Confirm selections** page, review the settings, and then select **Create**.
11. On the **View results** page, clear the **Create a volume when this wizard closes** check box, and then select **Close**.
12. In **Server Manager**, in the **navigation** pane, select **Volumes**.
13. In the **VOLUMES** area, select **TASKS**, and then select **New Volume**.
14. In the **New Volume Wizard**, on the **Before you begin** page, select **Next**.
15. On the **Select the server and disk** page, select **SEA-SVR3**, select **Three-Mirror**, and then select **Next**.
16. On the **Specify the size of the volume** page, select **Next**.
17. On the **Assign to a drive letter or folder** page, select **Drive letter**, select **T**, and then select **Next**.
18. On the **Select file system settings** page, in the **File system** drop-down list, select **ReFS**. In the **Volume label** text box, enter **TestData**, and then select **Next**.

19. On the **Confirm selections** page, select **Create**.
20. On the **Completion** page, select **Close**.
21. Close **Server Manager**.

18.3.3 Task 3: Copy a file to the volume, and verify visibility in File Explorer

1. Switch back to **SEA-SVR3**.
2. In the **Command Prompt** window, enter the following command, and then select Enter:

   ```
   netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
   ```

3. Return to **SEA-ADM1**.
4. In the taskbar, select the **File Explorer** icon.
5. In the **File Explorer** window, in the **Address bar**, enter **\\sea-svr3\t$**.
6. Right-click or access the context menu in the empty details pane, and then select **New Folder**. Name the folder **Test data**, and then select **Enter**.
7. Double-click **Test data**, or activate its context menu and select **Open**.
8. Right-click or access the context menu for the empty details pane, select **New**, and then **Text Document**. Name the new document **document1**, and then select **Enter**.

18.3.4 Task 4: Disconnect the disk and verify file availability

1. On **SEA-ADM1**, in Server Manager, in **File and Storage Services**, select **Storage Pools**, and then select **SP1**.
2. In the **Physical Disks** pane, select the **TASKS** drop-down list, and then select **Add Physical Disk**.
3. In the **Add Physical Disk** dialog box, in the **Allocation** drop-down list, ensure **Automatic** is selected, select the check box corresponding to the disk, and then select **OK**.
4. In the **PHYSICAL DISKS** pane, right-click the top disk in the list, and then select **Remove disk**.
5. In the **Remove Physical Disk** window, select **Yes**.
6. Review the statement in the **Remove Physical Disk** window, and then select **OK**.
7. Return to **File Explorer**.
8. Open **Document1.txt**, add some text, and then save and close the file.

18.3.5 Task 5: Add a new disk to storage pool

1. In Server Manager, on **SEA-ADM1**, in **File and Storage Services**, select **Storage Pools**.
2. In **Storage Pools**, in the **TASKS** drop-down list, select the **Rescan Storage** item.
3. In the **Rescan Storage** window, select **Yes**.
4. In the **Physical Disks** pane, select the **TASKS** drop-down list, and then select **Add Physical Disk**.
5. In the **Add Physical Disk** window, in the **Allocation** drop-down list, ensure **Automatic** is selected. Select the check box, and then select **OK**.
6. Return to File Explorer.
7. Open **Document1**, add some additional text, and then save and close the file.
8. Close all open windows.
9. Switch back to **SEA-SVR3**.
10. In the **Command Prompt** window, enter the following command, and then select Enter:

    ```
    T:

    Cd "test data"

    dir
    ```

11. Verify that **Document1.txt** is included in the returned results.
12. In the **Command Prompt** window, enter the following command, and then select Enter:

```
.\Document1.txt
```

13. When the document opens in **Notepad**, verify that all the text additions you made earlier are present, and then close **Notepad**.

    Note: When you have finished the exercise, revert the VMs to their initial state.

18.4 Exercise 4: Implementing Storage Spaces Direct

For Exercise 4, you will need to start the following VMs using the username **Contoso\Administrator**, and the password **Pa55w.rd**:

- WS-011T00A-SEA-DC1
- WS-011T00A-SEA-SVR1
- WS-011T00A-SEA-SVR2
- WS-011T00A-SEA-SVR3
- WS-011T00A-SEA-ADM1

18.4.1 Task 1: Install the features

1. On **SEA-ADM1**, in Server Manager, in the console tree, select **All Servers**, and verify that **SEA-SVR1**, **SEA-SVR2**, and **SEA-SVR3** have a **Manageability** of **Online – Performance counters not started** before continuing.
2. In Server Manager, in the **navigation** pane, select **File and Storage Services**, and then select **Disks**.
3. In the **Disks** pane, scroll until you find **SEA-SVR3** disks 1 through 4, and note that they are set to **Unknown**.
4. Right-click or access the context menu for each offline disk, select **Bring Online**, and then in the **Bring Disk Online** window, select **Yes**.
5. Verify that all disks are online for **SEA-SVR1** and **SEA-SVR2**.
6. Select **Start**, and in the **Start** menu, select **Windows PowerShell ISE**.
7. When **Windows PowerShell ISE** completes loading, select **File**, select **Open**, and then navigate to **C:\Labfiles\Mod04**.
8. Select **Implement-StorageSpacesDirect.ps1**, and then select **Open**.

   Note: The script is divided into numbered steps. There are eight steps, and each step has a number of commands. Run the commands by highlighting each command and pressing **F8**, one after the other in accordance with the following instructions.Ensure each step finishes, that is, goes from Stop operation (a red square) to a Run selection (green arrow) in the menu bar, before starting the next.

9. Select the line in step 1, that is, highlight the entire line, starting with the first **Invoke-Command**, and then select **F8**.
10. Wait until the installation finishes, and then verify that the output of the command includes four lines (one for each server) with **Success** as **True**.
11. Select the second line in step 1, starting with *second* **Invoke-Command**, and then select **F8**.

    Note: When you start the second command to restart the servers, you can run the third command to install the console without waiting for the second command's restarts to finish.

12. Select the third line in step 1, starting with **Install**, and then select **F8**.
13. Wait a few minutes while the servers restart and the **Failover Cluster Manager** tool is added to **SEA-ADM1**.
14. Leave the **Windows PowerShell ISE** console open for the remainder of the exercise.

18.4.2 Task 2: Create and validate a cluster

1. On **SEA-ADM1**, select the **Windows** key, and in the **Start** menu, select **Server Manager**.
2. In Server Manager, select **Tools**, and then select **Failover Cluster Manager**. (This is to confirm it is installed.) Leave the Server Manager console open.

3. In the **Administrator: Windows PowerShell ISE** window, select the line in step 2 starting with **Test-Cluster**, and then select **F8**.
4. Wait until the test finishes, which takes about 5 minutes.
5. Verify that the output of the command only includes warnings and that the last line is a validation report in HTML format.
6. In the **Administrator: Windows PowerShell ISE** window, select the line in step 3 starting with **New-Cluster**, and then select **F8**.
7. Wait until the installation finishes.
8. Verify that the output of the command only includes warnings, and that the last line has a **Name** column with the value **S2DCluster**.
9. Switch to the **Failover Cluster Manager** window, and in the **Management** pane, select **Connect to Cluster**, enter `S2DCluster.Contoso.com`, and then select **OK**.

18.4.3 Task 3: Enable Storage Spaces Direct

1. In the **Administrator: Windows PowerShell ISE** window, select the line in step 4 starting with **Invoke-Command**, and then select **F8**.
2. Wait until the installation finishes.
3. If a **Confirm** dialog box opens, select **Yes**.
4. There should be no output from the command, and ignore any warning message that opens.
5. In the **Administrator: Windows PowerShell ISE** window, select the line in step 5 starting with **Invoke-Command**, and then select **F8**.
6. Wait until the installation finishes.
7. In the output of the command, verify that the **FriendlyName** attribute has a value of **S2DStoragePool**.
8. In the **Failover Cluster Manager** window, expand `S2DCluster.Contoso.com`, expand **Storage**, and then select **Pools**.
9. Verify the existence of **Cluster Pool 1**.
10. In the **Administrator: Windows PowerShell ISE** window, select the line in step 6 starting with **Invoke-Command**, and then select **F8**.
11. Wait until the installation finishes.
12. Verify that in the output of the command is the attribute **FileSystemLabel**, with a value of **CSV**.
13. In the **Failover Cluster Manager** window, select **Disks**.
14. Verify the existence of **Cluster Virtual Disk (CSV)**.

18.4.4 Task 4: Create a storage pool, a virtual disk, and a share

1. In the **Administrator: Windows PowerShell ISE** window, select the line in step 7 starting with **Invoke-Command**, and then select **F8**.
2. Wait until the installation finishes.
3. Verify that in the output of the command is an attribute **FriendlyName**, with a value of **S2D-SOFS**. This validates that the command was successful.
4. In the **Failover Cluster Manager** window, select **Roles**.
5. Verify the existence of **S2D-SOFS**. This also verifies that the command was successful.
6. In the **Administrator: Windows PowerShell ISE** window, select the three lines in step 8, starting with **Invoke-Command**, and then select **F8**.
7. Wait until the installation finishes.
8. Verify that within the output of the command is an attribute **Path** with a value of **C:\ClusterStorage\CSV\VM01**. This validates that the command was successful.
9. In the **Failover Cluster Manager** window, select **S2D-SOFS**, and then select the **Shares** tab.
10. Verify the existence of **VM01**. This also verifies that the command was successful.

18.4.5 Task 5: Verify Storage Spaces Direct functionality

1. On **SEA-ADM1**, on the taskbar, select the **File Explorer** icon.
2. In **File Explorer**, in the address bar, enter **\\s2d-sofs\VM01**, and then select Enter.
3. Create a new folder named **VMFolder**, and then open it.
4. Switch to the **Administrator: Windows PowerShell ISE** window.
5. At the Windows PowerShell command prompt, enter the following command, and then select Enter:

   ```
   Stop-Computer -ComputerName SEA-SVR3
   ```

6. Switch to the **Server Manager** window, and then select **All Servers**.
7. In the **Servers** list, select **SEA-SVR3**.
8. Verify that **Manageability** changes to **Target computer not accessible**. **Note**: You may have to refresh the Server Manager view.
9. Switch back to the **File Explorer** window.
10. Create a new text document in the **VMFolder**.
11. In **Failover Cluster Manager**, select **Disks**, and then select **Cluster Virtual Disk (CSV)**.
12. Verify that for the **Cluster Virtual Disk (CSV)**, the **Health Status** is **Warning**, and **Operational Status** is **Degraded**. (**Operational Status** might also display as **Incomplete**.)
13. On the taskbar, select the **Microsoft Edge** icon.
14. In Microsoft Edge, in the Favorites menu, select the **Windows Admin Center (WAC)** tab.
15. In the **Windows security** window, in the **Username** text box, enter **Contoso\Administrator**, in the **Password** text box, enter **Pa55w.rd**, and then select **OK**.
16. In the **All connections** page, select **+ Add**.
17. In the **Add resources** blade, scroll to the **Windows Server cluster** pane, and in the pane, select **Add**.
18. In the **Add cluster** blade **Cluster name** text box, enter `S2DCluster.Contoso.com`, and then select **Add**.

    Note: Initially, the connection under the current user will be denied.
19. In the **Specify your credentials** window, select the **Use another account for this connection** radio button. In the **Username** text box, enter **Contoso\Administrator**, in the **Password** text box, enter **Pa55w.rd**, and then select Enter.
20. Clear the check box for **Also add servers in the cluster** (they are already included), and then select **Add**.
21. After the cluster is added to the **All connections** page, select `S2DCluster.Contoso.com`.
22. Verify that when the page loads, the **Dashboard** appears has an alert for **SEA-SVR3** being offline.
23. Start **WS-011T00A-SEA-SVR3**. (While **SEA-SVR3** should start quickly, it may take a few minutes for the alert to be removed.)

    When you have finished the exercise, revert the VMs to their initial state.

18.5 lab: title: 'Lab: Implementing and configuring virtualization in Windows Server' type: 'Answer Key' module: 'Module 5: Hyper-V virtualization and containers in Windows Server'

19 Lab answer key: Implementing and configuring virtualization in Windows Server

19.0.1 Exercise 1: Creating and configuring VMs

19.0.1.1 Task 1: Create a Hyper-V virtual switch

1. On SEA-ADM1, select **Start** and then select **Server Manager**.
2. In Server Manager, select **All Servers**.
3. In the Servers list, select and hold (or right-click) or access the context menu **SEA-SVR1** and then select **Hyper-V Manager**.
4. In Hyper-V Manager, ensure that `SEA-SVR1.Contoso.com` is selected.
5. In the Actions pane, select **Virtual Switch Manager**.
6. In the **Virtual Switch Manager**, in the **Create virtual switch** pane, select **Private** and then select **Create Virtual Switch**.
7. In the **Virtual Switch Properties** box, enter the following details and then select **OK**:
   - Name: **Contoso Private Switch**

- Connection type: **Private network**

19.0.1.2 Task 2: Create a virtual hard disk

1. On SEA-ADM1, in Hyper-V Manager, select **New** and then select **Hard Disk**. The **New Virtual Hard Disk Wizard** starts.
2. On the **Before you Begin page**, select **Next**.
3. On the **Choose Disk Format** page, select **VHD** and then select **Next**.
4. On the **Choose Disk Type** page, select **Differencing** and then select **Next**.
5. On the **Specify Name and Location** page enter the following and then select **Next**:
   - Name: **SEA-VM1**
   - Location: **C:\Base**
6. On the **Configure Disk** page, in the **Location** box, enter **C:\Base\BaseImage.vhd** and then select **Next**.
7. On the **Summary** page, select **Finish**.

19.0.1.3 Task 3: Create a virtual machine

1. On SEA-ADM1, in Hyper-V Manager, select **New** and then select **Virtual Machine**. The **New Virtual Machine Wizard** starts.
2. On the **Before you Begin page**, select **Next**.
3. On the **Specify Name and Location** page, enter **SEA-VM1** and then select the check box next to **Store the virtual machine in a different location**.
4. In the **Location** box, enter **C:\Base** and then select **Next**.
5. On the **Specify Generation** page, select **Generation 1** and then select **Next**.
6. On the **Assign Memory** page, enter **4096** and then select **Next**:
7. On the **Configure Networking** page, select the Connection drop-down menu, select **Contoso Private Switch** and then select **Next**.
8. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual hard disk**, and then select **Browse**.
9. Browse to **C:\Base**, select **SEA-VM1.vhd**, select **Open** and then select **Next**.
10. On the **Summary** page, select **Finish**. Notice that SEA-VM1 displays in the Virtual Machines list.
11. Select **SEA-VM1** and then in the Actions pane, under SEA-VM1, select **Settings**.
12. In the **Hardware** list, select **Memory**.
13. In the **Dynamic Memory** section, select the check box next to **Enable Dynamic Memory**.
14. Next to **Maximum RAM**, enter **4096** and then select **OK**.
15. Close Hyper-V Manager.

19.0.2 Task 4: Manage Virtual Machines using Windows Admin Center

1. On SEA-ADM1, on the taskbar, select **Microsoft Edge**.
2. In Microsoft Edge, on the Favorites Bar, select **Windows Admin Center**.
3. In the Windows Security box, enter **Contoso\Administrator** with the password of **Pa55w.rd** and then select **OK**.
4. In the **All connections** list, select **SEA-SVR1**.

   Note: You may need to select **Manage As** to then enter the credentials in the next step.
5. In the **Specify your credentials** page, select **Use another account for this connection**, and then enter **Contoso\Administrator** with the password of **Pa55w.rd**.
6. In the **Tools** list, select **Virtual Machines**. Review the Summary pane.
7. Select the **Inventory** tab. Notice the two virtual machines.
8. Select **SEA-VM1**. Review the **Properties** pane.
9. Select **Settings** and then select **Disks**.
10. Select **Add disk**.
11. Select **Create an empty virtual hard disk** and then in the Size box enter **5** GB.
12. Select **Save disks settings** and then select **Close**.

Note: The **Save Disk** Setting may be greyed out which is a known issue. A workaround would be to create the disk in Hyper-V if needed.

13. On the **Properties** page, select **Start** to start **SEA-VM1**.
14. Scroll down and display the statistics for the running VM.
15. Refresh the page and then select **Shut down**. Select **Yes** to confirm.
16. In the **Tools** list, select **Virtual switches**. Notice the two switches that have been configured.
17. Close all open windows on SEA-ADM1.

19.0.3 Exercise 1 results

After this exercise, you should have used Hyper-V Manager and Windows Admin Center to create a virtual switch, create a virtual hard disk, and then create and manage a virtual machine.

19.0.4 Exercise 2: Installing and configuring containers

19.0.4.1 Task 1: Install Docker on Windows Server

1. On SEA-ADM1, from the taskbar, open **Microsoft Edge**.
2. On the Favorites bar, select **Windows Admin Center**.
3. In the Windows Security box, enter the following credentials:
   - User name: **Contoso\Administrator**
   - Password: **Pa55w.rd**
4. On the **All connections** page, select **SEA-SVR1**.
5. On the **Specify your credentials** page, select **Use another account for this connection**. Provide the **Contoso\Administrator** credentials, and then select **Continue**.
6. In the **Tools** list, select **PowerShell**. Provide the **Contoso\Administrator** credentials, and then select **Enter**. You are now connected to SEA-SVR1 using a Remote PowerShell connection.

   Note: The Powershell connection in **WAC** may be slow due to nested virtualization used in the lab, so an alternate method is to use **Enter-PSSession -computername SEA-SVR1** from a Powershell window on **SEA-ADM1**.
7. At the PowerShell command prompt enter the following command and then select Enter:

   ```
   Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
   ```
8. At the NuGet Provider prompt, enter **Y** for yes and then select Enter.
9. At the PowerShell command prompt enter the following command and then select Enter:

   ```
   Install-Package -Name docker -ProviderName DockerMsftProvider
   ```
10. At the confirmation prompt, enter **A** for Yes to All and then select Enter.
11. After the installation is complete, restart the computer by using the following command:

    ```
    Restart-Computer -Force
    ```

19.0.4.2 Task 2: Install and run a Windows container

1. After SEA-SVR1 restarts reconnect the PowerShell tool and provide the Contoso\Administrator credentials.
2. Verify the installed version of Docker by using the following command:

   ```
   Get-Package -Name Docker -ProviderName DockerMsftProvider
   ```

   Note: You may need to run **Start-Service -name Docker** before running the next commands.
3. To verify whether any Docker images are currently pulled, use the following command:

   ```
   Docker images
   ```

   Notice that there are no images in the local repository store.

4. To review docker base images from the online Microsoft repository, use the following command:

   ```
   Docker search Microsoft
   ```

   Notice the variety of base images each representing various runtime scenarios.

   Note: You may disregard any errors and continue with the next step.

5. To download a server core image, with IIS, that matches the host operating system, run the following command:

   ```
   docker pull mcr.microsoft.com/windows/servercore/iis:windowsservercore-ltsc2019
   ```

   Note: This download may take more than 15 minutes to complete.

6. To confirm the Docker image that is currently pulled, use the following command:

   ```
   Docker images
   ```

   Notice that there is now an image listed in the local repository store.

7. To run the container, enter the following command:

   ```
   Docker run -d -p 80:80 --name ContosoSite mcr.microsoft.com/windows/servercore/iis:windowsserverco
   cmd
   ```

   This command runs the IIS image as a background service (-d) and configures networking such that port 80 of the container host maps to port 80 of the container.

8. Enter the following command to retrieve the IP address information of the container host:

   ```
   ipconfig
   ```

   Note the IPv4 address of the Ethernet adapter named vEthernet (nat). This is the address of the new container. Make a note of the IPv4 address of the Ethernet adapter named **Ethernet**. This is the IP address of the Host (SEA-SVR1).

9. In Microsoft Edge, open another tab and then enter `<http://172.16.10.12>`. Observe the default IIS page.

10. In the remote PowerShell session, enter the following command:

    ```
    docker ps
    ```

    This command provides information on the container that is currently running on SEA-SVR1. Take note of the container ID as you will use it to stop the Container.

11. In the remote PowerShell session, enter the following command:

    ```
    docker stop <ContainerID>
    ```

12. Rerun the `docker ps` command to confirm that the container has stopped.

19.0.4.3 Task 3: Use Windows Admin Center to manage containers

1. On SEA-ADM1, ensure that SEA-SVR1 is targeted in the Windows Admin Center and then select the **Containers** tool.
2. Browse through each of the **Summary**, **Containers**, **Images**, **Networks**, and **Volumes** tabs.

19.0.5 Exercise 2 results

19.1 After this exercise, you should have installed Docker on Windows Server and installed and run a Windows container containing web services.

19.2 lab: title: 'Lab: Implementing failover clustering' type: 'Answer Key' module: 'Module 6: High availability in Windows Server'

20 Lab answer key: Implementing failover clustering

20.1 Exercise 1: Configuring iSCSI storage

20.1.1 Task 1: Install Failover Clustering

1. On **SEA-ADM1**, select **Start**, right-click or access the context menu for **Windows PowerShell**, and then select **Run as Administrator**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
   ```

3. Wait until the installation process is complete and a command prompt appears.
4. On **SEA-ADM1**, repeat step 1 to open a new PowerShell session that you'll use to connect to the **SEA-SVR2** server.
5. In the new **Administrator:Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   $cred=Get-Credential
   ```

6. When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
7. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   $sess = New-PSSession -Credential $cred -ComputerName sea-svr2.contoso.com
   ```

8. After running the previous command, enter the following command, and then select Enter:

   ```
   Enter-PSSession $sess
   ```

9. Verify that `sea-svr2.contoso.com` appears at the beginning of the command prompt.
10. In the **Administrator: Windows PowerShell** window for **SEA-SVR2**, enter the following command, and then select Enter:

    ```
    Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
    ```

11. On **SEA-ADM1**, repeat step 1 to open a new PowerShell session that you'll use to connect to the **SEA-SVR3** server.
12. To install the Failover Clustering feature on **SEA-SVR3**, in the new **Administrator: Windows PowerShell** window, enter the following command, and then select Enter.

    ```
    $cred=Get-Credential
    ```

13. When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
14. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    $sess = New-PSSession -Credential $cred -ComputerName sea-svr3.contoso.com
    ```

15. After running the previous command, enter the following command, and then select Enter:

    ```
    Enter-PSSession $sess
    ```

16. Verify that `sea-svr3.contoso.com` appears at the beginning of the command prompt.
17. In the **Administrator: Windows PowerShell** window for **SEA-SVR3**, enter the following command, and then select Enter:

```
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

18. On **SEA-ADM1**, in the **Administrator: Windows PowerShell** window for the local server, enter the following command, and then select Enter:

    ```
    Add-WindowsFeature FS-iSCSITarget-Server
    ```

19. Wait until the installation finishes and the command prompt returns.
20. In the PowerShell window for **SEA-SVR2**, enter the following command, and then select Enter:

    ```
    Restart-Computer
    ```

21. In the PowerShell window for **SEA-SVR3**, enter the following command, and then select Enter:

    ```
    Restart-Computer
    ```

22. In the PowerShell window for **SEA-ADM1**, enter the following command, and then select Enter:

    ```
    Restart-Computer
    ```

23. Wait for 3–4 minutes for all three servers to restart.

20.1.2 Task 2: Configure iSCSI virtual disks

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with password **Pa55w.rd**.
2. Select **Start**, right-click or access the context menu for **Windows PowerShell**, and then select **Run as Administrator**.
3. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    New-IscsiVirtualDisk c:\Storage\disk1.VHDX -size 10GB
    ```

4. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    New-IscsiVirtualDisk c:\Storage\disk2.VHDX -size 10GB
    ```

5. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    New-IscsiVirtualDisk c:\Storage\disk3.VHDX -size 10GB
    ```

6. To open another **Windows PowerShell** window to connect to **SEA-SVR2**, on **SEA-ADM1**, select **Start**, right-click or access the context menu for **Windows PowerShell**, and then select **Run as Administrator**.
7. In the new **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    $cred=Get-Credential
    ```

8. When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
9. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    $sess = New-PSSession -Credential $cred -ComputerName sea-svr2.contoso.com
    ```

10. After running the previous command, enter the following command, and then select Enter:

    ```
    Enter-PSSession $sess
    ```

11. Verify that **sea-svr2.contoso.com** appears at the beginning of the command prompt.
12. To open another **Windows PowerShell** window to connect to **SEA-SVR3**, on **SEA-ADM1**, select **Start**, right-click or access the context menu for **Windows PowerShell**, and then select **Run as Administrator**.
13. In the new **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    $cred=Get-Credential
    ```

14. When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
15. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

```
$sess = New-PSSession -Credential $cred -ComputerName sea-svr3.contoso.com
```

16. After running the previous command, enter the following command, and then select Enter:

```
Enter-PSSession $sess
```

17. Verify that **sea-svr3.contoso.com** appears at the beginning of the command prompt.

> **Note:** You should have three **Windows PowerShell** windows opened. Ensure that you always use the proper PowerShell session window that's connected to the server where you want to run a command.

18. In the **Administrator: Windows PowerShell** window for **SEA-SVR2**, start the Microsoft iSCSI Initiator service by entering the following commands, each followed by selecting Enter:

```
Start-Service msiscsi

Set-Service msiscsi -startuptype "automatic"
```

19. In the **Administrator: Windows PowerShell** window for **SEA-SVR3**, start the Microsoft iSCSI Initiator service by entering the following commands, each followed by selecting Enter:

```
Start-Service msiscsi

Set-Service msiscsi -startuptype "automatic"
```

20. On **SEA-ADM1**, in the **Administrator: Windows PowerShell** window for the local machine, enter:

```
New-IscsiServerTarget iSCSI-MOD6 -InitiatorIds "IQN:iqn.1991-05.com.microsoft:sea-svr2.contoso.com
```

20.1.3 Results

After completing this exercise, you should have successfully installed the Failover Clustering feature and configured the Internet SCSI (iSCSI) Target Server.

20.2 Exercise 2: Configuring a failover cluster

20.2.1 Task 1: Connect clients to the iSCSI targets

1. In the PowerShell window for **SEA-ADM1**, enter each of the following commands, each followed by selecting Enter:

```
Add-IscsiVirtualDiskTargetMapping iSCSI-MOD6 c:\Storage\Disk1.VHDX

Add-IscsiVirtualDiskTargetMapping iSCSI-MOD6 c:\Storage\Disk2.VHDX

Add-IscsiVirtualDiskTargetMapping iSCSI-MOD6 c:\Storage\Disk3.VHDX
```

2. In the **Administrator: Windows PowerShell** window for **SEA-SVR2**, enter the following commands, and after each, select Enter:

```
New-iSCSITargetPortal -TargetPortalAddress SEA-ADM1.contoso.com

Connect-iSCSITarget -NodeAddress iqn.1991-05.com.microsoft:sea-adm1-iscsi-mod6-target

Get-iSCSITarget | fl
```

3. Verify that after running the last command, the value for the *IsConnected* variable is True.
4. In the **Administrator: Windows PowerShell** window for **SEA-SVR3**, enter the following commands, and then select Enter after each:

```
New-iSCSITargetPortal -TargetPortalAddress SEA-ADM1.contoso.com

Connect-iSCSITarget -NodeAddress iqn.1991-05.com.microsoft:sea-adm1-iscsi-mod6-target
```

```
Get-iSCSITarget | fl
```

5. Verify that after you run the last command, the value for the *IsConnected* variable is True.

20.2.2 Task 2: Initialize the disks

1. In the **Administrator: Windows PowerShell** window for **SEA-SVR2**, enter the following command, and then select Enter:

   ```
   Get-Disk
   ```

2. After running this command, ensure that three disks are in the **Offline** operational status. These should be disks with numbers 4, 5, and 6.

3. In the **Administrator: Windows PowerShell** window for **SEA-SVR2**, enter the following commands, selecting Enter after each:

   ```
   Get-Disk | Where OperationalStatus -eq 'Offline' | Initialize-Disk -PartitionStyle MBR

   New-Partition -DiskNumber 4 -Size 5gb -AssignDriveLetter

   New-Partition -DiskNumber 5 -Size 5gb -AssignDriveLetter

   New-Partition -DiskNumber 6 -Size 5gb -AssignDriveLetter

   Format-Volume -DriveLetter E -FileSystem NTFS

   Format-Volume -DriveLetter F -FileSystem NTFS

   Format-Volume -DriveLetter G -FileSystem NTFS
   ```

20.2.3 Task 3: Validate and create a failover cluster

1. Switch to **SEA-SVR2**, and then sign in as **Contoso\Administrator** with password **Pa55w.rd**.

   > **Note:** You must sign in on **SEA-SVR2** because you can't run cluster commands over remote PowerShell.

2. Enter **PowerShell**, and then select Enter.

3. At the command prompt on **SEA-SVR2**, enter **Test-Cluster SEA-SVR2, SEA-SVR3**, and then select Enter.

4. Wait for a few minutes for the cluster validation test to complete. You can expect a few warning messages to appear, but there should be no errors.

5. At the command prompt on **SEA-SVR2**, enter the following command, and then select Enter:

   ```
   New-Cluster -Name WFC2019 -Node sea-svr2 -StaticAddress 172.16.10.125
   ```

6. You should receive a cluster name as a result. It should display **Name WFC2019**. Verify that there are no errors.

7. At the command prompt on **SEA-SVR2**, enter the following command, and then select Enter:

   ```
   Add-ClusterNode -Name SEA-SVR3
   ```

8. When a command prompt appears, verify that no errors are reported.

20.2.4 Results

After completing this exercise, you should have installed and configured the Failover Clustering feature.

20.3 Exercise 3: Deploying and configuring a highly available file server

20.3.1 Task 1: Add the file server application to the failover cluster

1. On **SEA-ADM1**, open **Server Manager**, and then select **Failover Cluster Manager** in the **Tools** menu.

2. In the **Failover Cluster Manager** console, select **Connect to Cluster**.
3. To connect to the cluster that you created in the previous exercise, in the **Select Cluster** window, enter **WFC2019**, and then select **OK**.
4. Expand `WFC2019.contoso.com`, select **Roles**, and then notice that no roles display. This is because no cluster roles are configured yet.
5. Select **Nodes**, and then notice that the **SEA-SVR2** and **SEA-SVR3** nodes both display a status of **Up**.
6. Expand **Storage**, and then select **Disks**. Notice that three cluster disks have a status of **Online**.
7. On the **Failover Cluster Manager** page, right-click or access the context menu for **Roles**, and then select **Configure role**.
8. On the **Before You Begin** page, select **Next**.
9. On the **Select Role** page, select **File Server**, and then select **Next**.
10. On the **File Server Type** page, select **File Server for general use**, and then select **Next**.
11. On the **Client Access Point** page, in the **Name** box, enter **FSCluster**.
12. In the **Address** box, enter **172.16.10.130**, and then select **Next**.
13. On the **Select Storage** page, select **Cluster Disk 1** and **Cluster Disk 2**, and then select **Next**.
14. On the **Confirmation** page, select **Next**.
15. On the **Summary** page, select **Finish**.
16. In the **Storage** node, select **Disks**.
17. Verify that three cluster disks are online. **Cluster Disk 1** and **Cluster Disk 2** should be assigned to **FSCluster**.

20.3.2 Task 2: Add a shared folder to a highly available file server

1. On **SEA-ADM1**, in **Failover Cluster Manager**, select **Roles**, select **FSCluster**, and then in the right pane, select **Add File Share**.
2. On the **Select Profile** page, select **SMB Share - Quick**, and then select **Next**.
3. On the **Share Location** page, select **Next**.
4. On the **Share Name** page, enter **Docs** for the share name, and then select **Next**.
5. On the **Other Settings** page, select **Next**.
6. On the **Permissions** page, select **Next**.
7. On the **Confirmation** page, select **Create**.
8. On the **View results** page, select **Close**.

20.3.3 Task 3: Configure the failover and failback settings

1. **On SEA-ADM1**, in the **Failover Cluster Manager** console, select **Roles**, select **FSCluster**, and then select **Properties**.
2. Select the **Failover** tab, and then select **Allow failback**.
3. Select **Failback between**, and then enter:
   - **4** in the first text box
   - **5** in the second text box.
4. Select the **General** tab.
5. Under **Preferred owners**, select both **SEA-SVR2** and **SEA-SVR3**.
6. Select the **SEA-SVR3** object, select **Up**, and then select **OK**.

20.3.4 Results

After completing this exercise, you should have configured a highly available file server.

20.4 Exercise 4: Validating the deployment of the highly available file server

20.4.1 Task 1: Validate the highly available file server deployment

1. On **SEA-ADM1**, open File Explorer, and then try to access the **\\FSCluster** location.
2. Verify that you can access the **Docs** folder.
3. Inside the **Docs** folder, right-click or access the context menu in an empty area of the folder, select **New**, and then select **Text Document**.
4. To accept the default name of the document as **New Text Document.txt**, select Enter.
5. In the **Failover Cluster Manager** console, right-click or access the context menu for **FSCluster**, select **Move**, select **Select node**, choose the available node from the **Cluster nodes** list, and then select **OK**.
6. On **SEA-ADM1**, in File Explorer, verify that you can still access the **\\FSCluster** location.

20.4.2 Task 2: Validate the failover and quorum configuration for the File Server role

1. On **SEA-ADM1**, in **Failover Cluster Manager**, determine the current owner for the **FSCluster** role. If you select **Roles** and observe the value in the **Owner Node** column, it will be **SEA-SVR2** or **SEA-SVR3**.
2. Select **Nodes**, and then right-click or access the context menu for the node that's the current owner of the **FSCluster** role.
3. Select **More Actions**, and then select **Stop Cluster Service**.
4. Try to access **FSCluster** from **SEA-ADM1** to verify that **FSCluster** has moved to another node and that the **FSCluster** location is still available.
5. Select **Nodes**, and then right-click or access the context menu for the node that has the status of **Down**.
6. Select **More Actions**, and then select **Start Cluster Service**.
7. In the **Failover Cluster Manager** console, right-click or access the context menu for the `WFC2019.Contoso.com` cluster, select **More Actions**, and then select **Configure Cluster Quorum Settings**.
8. On the **Before you begin** page, select **Next**.
9. On the **Select Quorum Configuration Options** page, select **Use default quorum configuration**, and then select **Next**.
10. Select **Next**, and then select **Finish**.
11. Browse to the **Disks** node, select the disk marked **witness disk in Quorum**, and then select **Take Offline**.
12. When prompted, select **Yes**.
13. Verify that **FSCluster** is still available by trying to access it from **SEA-ADM1**.
14. Select the disk marked **witness disk in Quorum**, and then select **Bring Online**.
15. Close all open windows.

20.4.3 Results

20.5 After completing this exercise, you should have validated high availability with Failover Clustering.

20.6 lab: title: 'Lab: Implementing Hyper-V Replica and Windows Server Backup' type: 'Answer Key' module: 'Module 7: Disaster Recovery in Windows Server'

21 Lab answer key: Implementing Hyper-V Replica and Windows Server Backup

21.1 Exercise1: Implementing Hyper-V Replica

21.1.1 Task 1: Configure a replica on both host machines

1. On **SEA-ADM1**, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
2. Select **Start**, and then enter **powershell**. Right-click or access the context menu for Windows PowerShell, and then select **Run as administrator**.
3. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   $cred=Get-Credential
   ```

   When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
4. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   $sess = New-PSSession -Credential $cred -ComputerName sea-svr1.contoso.com
   ```

   Next, enter the following command, and then select Enter:

   ```
   Enter-PSSession $sess
   ```

   You should get a [`sea-svr1.contoso.com`] title in your command prompt. From this point, all the commands that you enter run on **SEA-SVR1**.

5. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Get-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"
   ```

   You'll receive the properties of this firewall rule. Search for the value of the *Enabled* variable. It should be set to **False**. To enable **SEA-SVR1** as a replication host, you must enable this firewall rule.

6. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"
   ```

7. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Get-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener (TCP-In)"
   ```

   You'll receive the properties of this firewall rule. Search for the value of the *Enabled* variable. Now it should be set to **True**.

8. To configure **SEA-SVR1** as a Replica server for **Hyper-V Replica**, enter the following command in the PowerShell window, and then select Enter:

   ```
   Set-VMReplicationServer -ReplicationEnabled $true -AllowedAuthenticationType Kerberos -ReplicationA
   ```

9. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Get-VMReplicationServer
   ```

   You should get the configuration setting that you configured in the previous step, which is as follows:

   - **RepEnabled:True**
   - **AuthType:Kerb**
   - **KerAuthPort:80**
   - **CertAuthPort:443**
   - **AllowAnyServer:True**

10. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    Get-VM
    ```

    SEA-CORE1 should be listed as a virtual machine (VM) that's configured on this Hyper-V server. Leave the **Administrator: Windows PowerShell** window open.

11. Select **Start**, and then enter **powershell**. Right-click or access the context menu for Windows PowerShell, and then select **Run as administrator**. This will open another instance of Windows PowerShell.

12. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    $cred=Get-Credential
    ```

    When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

13. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    $sess1 = New-PSSession -Credential $cred -ComputerName sea-svr2.contoso.com
    ```

    Next, enter the following command, and then select Enter:

    ```
    Enter-PSSession $sess1
    ```

    You should get a [`sea-svr2.contoso.com`] title in your command prompt. From this point, all commands that you enter run on **SEA-SVR2**.

14. Repeat steps 5 through 10 in the PowerShell window where you have a session opened on `sea-svr2.contoso.com`. This will configure **SEA-SRV2** for **Hyper-V Replica**. In step 10, you should get no result when running the **Get-VM** command because no VMs are configured on **SEA-SVR2**.

15. Leave both PowerShell sessions open for the next task.

21.1.2 Task 2: Configure replication

1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following command, and then select Enter:

   ```
   Enable-VMReplication SEA-CORE1 -ReplicaServerName SEA-SVR2.contoso.com -ReplicaServerPort 80 -Auth
   ```

2. After you have verified that you didn't receive any error message from the previous command, enter the following command, and then select Enter:

   ```
   Start-VMInitialReplication SEA-CORE1
   ```

   This starts the initial replication process for VM **SEA-CORE1**, from **SEA-SVR1** to **SEA-SVR2**.

3. After you have verified that you didn't receive any error message from the previous command, enter the following command, and then select Enter:

   ```
   Get-VMReplication
   ```

   This command retrieves the replication status.

   In the result table, search for the value in the **State** column. It should be **InitialReplicationInProgress**. Wait for 4–5 minutes, and then repeat this command. Verify that the value in the **State** column is **Replicating**. Don't proceed to the next steps until you get this value. Additionally, ensure that **Primary server** is set to **SEA-SVR1** and **ReplicaServer** is set to **SEA-SVR2**.

4. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   get-vm
   ```

   Verify that you now have the **SEA-CORE1** VM on **SEA-SVR2**. This means that the VM successfully replicated.

5. Leave both Windows PowerShell sessions open for the next task.

21.1.3 Task 3: Validate failover

1. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following command, and then select Enter:

   ```
   Start-VMFailover -Prepare -VMName SEA-CORE1 -computername SEA-SVR1.contoso.com
   ```

   When prompted, enter **Y**, and then select Enter. This command prepares for the planned failover of **SEA-CORE1** by replicating any pending changes.

2. Switch to the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Start-VMFailover -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com
   ```

   When prompted, enter **Y**, and then select Enter. This command fails over the replica VM.

3. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Set-VMReplication -Reverse -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com
   ```

   This command switches the replica VM to a primary VM.

4. In the PowerShell window where you have the remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Start-VM -VMName SEA-CORE1 -computername SEA-SVR2.contoso.com
   ```

   This command starts the VM that has been switched from a replica VM to a primary VM.

5. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Get-VM
   ```

In the result table, search for the value in the **State** column. It should be **Running**.

6. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Get-VMReplication
   ```

   In the result table, search for the value in the **State** column. It should be **Replicating**. Additionally, ensure that the **Primary server** is now set to **SEA-SVR2** and that **ReplicaServer** is set to **SEA-SVR1**.

7. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following command, and then select Enter:

   ```
   Stop-VM SEA-CORE1
   ```

8. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following commands, and then select Enter:

   ```
   Exit-PSSession
   Remove-PSSession $sess
   ```

9. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr2.contoso.com**, enter the following commands, and then select Enter:

   ```
   Exit-PSSession
   Remove-PSSession $sess1
   ```

10. Close both PowerShell windows and leave the VMs running.

    Note: If you want to verify the results of this exercise by using GUI tools, you can start Hyper-V Manager on **SEA-ADM1**, and then add the **SEA-SVR1** and **SEA-SVR2** servers to the **Hyper-V** console. You can then verify that the **SEA-CORE1** VM exists on both **SEA-SVR1** and **SEA-SVR2** and that replication is running from **SEA-SVR2** to **SEA-SVR1**.

Results: After completing this exercise, you should have configured **Hyper-V Replica** and tested failover.

21.2 Exercise 2: Implementing backup and restore with Windows Server Backup

21.2.1 Task1: Configure Windows Server Backup options

1. If necessary, sign in to **SEA-ADM1** as **Contoso\Administrator** with password **Pa55w.rd**.
2. Select **File Explorer** on the taskbar.
3. In the **File Explorer** window, select **Local Disk (C:)** in the **navigation** pane.
4. Right-click or access the context menu in an empty space in the **details** pane, select **New**, and then select **Folder**. You can also open **File Explorer**, select the **Home** menu, and then select the **New Folder** option.
5. Name the folder **BackupShare**. Right-click or access the context menu for the **BackupShare** folder, select **Give access to**, and then select **Specific people**.
6. In the **Network access** window, enter **Authenticated Users**, and then select **Add**. In the **Permission Level** column, set the value for **Authenticated Users** to **Read/Write**, select **Share**, and then select **Done**.
7. Select **Start**, and then enter **powershell**. Right-click or access the context menu for Windows PowerShell, and then select **Run as administrator**.
8. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   $cred=Get-Credential
   ```

   When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

9. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   $sess = New-PSSession -Credential $cred -ComputerName sea-svr1.contoso.com
   ```

Next, enter the following command, and then select Enter:

```
Enter-PSSession $sess
```

You should get a [sea-svr1.contoso.com] title in your command prompt. From this point, all commands that you enter run on **SEA-SVR1**.

10. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    Import-Module Servermanager
    ```

    Next, enter the following command, and then select Enter:

    ```
    Get-WindowsFeature Windows-Server-Backup
    ```

    Ensure that the **Install State for Windows Server Backup** feature is **Available**.

11. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    Install-WindowsFeature Windows-Server-Backup
    ```

    Wait until you get the result. Ensure that **True** displays in the **Success** column.

12. Repeat the command:

    ```
     Get-WindowsFeature Windows-Server-Backup
    ```

    Ensure that the **Install State for Windows Server Backup** feature is now **Installed**.

13. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    wbadmin /?
    ```

    You'll get the list of commands that are available for the Windows Server Backup command-line tool.

14. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:

    ```
    Get-Command -Module WindowsServerBackup -CommandType Cmdlet
    ```

    You'll get a list of available PowerShell cmdlets for Windows Server Backup.

21.2.2 Task 2: Perform a backup

1. In the PowerShell window where you have a remote PowerShell session opened for **sea-svr1.contoso.com**, enter the following commands, and then select Enter:

    ```
    $Policy = New-WBPolicy
    $Filespec = New-WBFileSpec -FileSpec "C:\Files"
    ```

2. After you have run the commands from the previous step, where you defined variables for the backup policy and the file path to back up, add this to the backup policy by entering the following command, and then selecting Enter:

    ```
    Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec
    ```

3. Now, you must configure a backup location on the **SEA-AD1** network share by entering the following commands, and then selecting Enter:

    ```
    $Cred = Get-Credential
    $NetworkBackupLocation = New-WBBackupTarget -NetworkPath "\\SEA-ADM1\BackupShare" -Credential $Cre
    ```

    Note: When prompted, sign in as **Contoso\Administrator** with password **Pa55w.rd**.

4. Now you must add this backup location to the backup policy by entering the following command, and then selecting Enter (if prompted, enter Y, and then select Enter):

    ```
    Add-WBBackupTarget -Policy $Policy -Target $NetworkBackupLocation
    ```

5. Before starting a backup job, you must configure more options to enable Volume Shadow Copy Service backups by entering the following command, and then selecting Enter:

```
Set-WBVssBackupOptions -Policy $Policy -VssCopyBackup
```

6. To start a backup job, in order to back up the content of the **C:\Files** folder on **SEA-SVR1** to a network share on **SEA-ADM1**, you must enter the following command, and then select Enter:

   ```
   Start-WBBackup -Policy $Policy
   ```

   Wait until you receive the "The backup operation completed" message.

7. On **SEA-ADM1**, open File Explorer, and then browse to **C:\BackupShare**. Open the folder, and then ensure that the backup files are there.

8. Close all PowerShell windows.

21.3 Results: After completing this exercise, you should have configured Windows Server Backup and performed a backup on SEA-SVR1.

21.4 lab: title: 'Lab: Configuring security in Windows Server' type: 'Answer Key' module: 'Module 8: Windows Server security'

22 Lab answer key: Configuring security in Windows Server

22.1 Exercise 1: Configuring Windows Defender Credential Guard

Note: In the lab environment, Credential Guard will not run VMs because they don't meet the requirements. You can still create the GPO (Group Policy Objects) and run the tool.

22.1.1 Task 1: Enable Windows Defender Credential Guard using Group Policy

1. Sign-in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start**, and then enter **Group Policy Management**.
3. Select **Group Policy Management**.
4. In the Group Policy Management Console, expand **Forest: `Contoso.com`**, expand **Domains**, expand `Contoso.com`, right-click or access the context menu for the **IT** OU (Organizational Unit), and then select **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** dialog box, in the **Name** text box, enter **CredentialGuard_GPO**, and then select **OK**.
6. In the **Group Policy Management** window, under **IT**, right-click or access the context menu for **CredentialGuard_GPO**, and then select **Edit**.
7. In the Group Policy Management Editor, navigate to **Computer Configuration\Policies\Administrative Templates\System\Device Guard**.
8. Select **Turn On Virtualization Based Security**, and then select the **policy setting** link.
9. Select **Enabled**.
10. In the **Select Platform Security Level** drop-down list, select **Secure Boot and DMA Protection**.
11. In the **Credential Guard Configuration** drop-down list, select **Enabled with UEFI lock**.
12. In the **Secure Launch Configuration** drop-down list, select **Enabled**, and then select **OK**.
13. Close the Group Policy Management Editor.
14. Close the Group Policy Management Console.

22.1.2 Task 2: Enable Windows Defender Credential Guard using the Hypervisor-Protected Code Integrity and Windows Defender Credential Guard hardware readiness tool

1. On **SEA-ADM1**, select **Start**, and then enter **Powershell**.

2. Right-click or access the context menu for **Windows PowerShell**, and then select **Run as administrator**.

3. Navigate to **c:\labfiles\Mod08**.

4. Enter the following command:

   ```
   DG_Readiness_Tool.ps1 -Enable -AutoReboot
   ```

5. Your virtual machine will restart after the tool has completed running.

6. When the virtual machine restarts, reenter the credentials for **Contoso\Administrator**.

22.2 Exercise 2: Locating problematic accounts

22.2.1 Task 1: Locate and reconfigure accounts with passwords that don't expire

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Open Windows PowerShell.
3. Enter the following command:

   ```
   Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true}
   ```

4. Review the list of user accounts returned.
5. Enter the following command:

   ```
   Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true} | Set-ADUser -PasswordN
   ```

6. Rerun the command from step 3 and notice that no users are returned.

22.2.2 Task 2: Locate and disable accounts to which no sign-ins have occurred for at least 90 days

1. Enter the following commands:

   ```
   $days = (Get-Date).Adddays(-90)
   Get-ADUser -Filter {LastLogonTimeStamp -lt $days -and enabled -eq $true} -Properties LastLogonTime
   ```

2. In the lab environment, no accounts will be returned.
3. Enter the following command:

   ```
   Get-ADUser -Filter {LastLogonTimeStamp -lt $days -and enabled -eq $true} -Properties LastLogonTime
   ```

4. No results will be returned in the lab environment.

22.3 Exercise 3: Implementing LAPS

22.3.1 Task 1: Prepare OU and computer accounts for LAPS (Local Administrator Password Solution)

1. Sign in to **SEA-ADM1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Open Windows PowerShell.
3. Enter the following commands:

   ```
   New-ADOrganizationalUnit -Name "Seattle_Servers"
   Get-ADComputer SEA-SVR1 | Move-ADObject -TargetPath "OU=Seattle_Servers,DC=Contoso,DC=com"
   ```

4. Enter the following command:

   ```
   Msiexec /I C:\Labfiles\Mod08\LAPS.x64.msi
   ```

5. When the **Local Administrator Password Solution Setup Wizard** opens, select **Next**.
6. Select **I accept the terms in the License Agreement**, and then select **Next**.
7. Under **Custom Setup**, in the drop-down menu next to **Management Tools**, select **Entire feature will be installed on the local hard drive**.
8. Select **Next**, select **Install**, and then select **Finish**.

22.3.2 Task 2: Prepare AD DS (Active Directory) for LAPS

1. In Windows PowerShell, enter the following commands:

   ```
   Import-Module admpwd.ps
   Update-AdmPwdADSchema
   Set-AdmPwdComputerSelfPermission -Identity "Seattle_Servers"
   ```

2. Select **Start**, and then enter **Group Policy**.
3. Select **Group Policy Management**.

4. In the Group Policy Management Console, expand **Forest: `Contoso.com`**, expand **Domains**, expand **`Contoso.com`**, right-click or access the context menu for the **Seattle_Servers** OU, and then select **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** dialog box, in the **Name** text box, enter **LAPS_GPO**, and then select **OK**.
6. In the **Group Policy Management** window, under **Seattle_Servers**, right-click or access the context menu for **LAPS_GPO**, and then select **Edit**.
7. In the **Group Policy Management Editor** window, under **Computer Configuration**, expand the **Policies** node, expand the **Administrative Templates** node, and then select **LAPS**.
8. Select the **Enable local admin password management** policy, and then select the **policy settings** link.
9. In the **Enable local admin password management** window, select **Enabled**, and then select **OK**.
10. Select the **Password Settings** policy, and then select the **policy settings** link.
11. In the **Password Settings** policy dialog box, select **Enabled**, and then configure **Password Length** to **20**.
12. Verify that the **Password Age (Days)** is configured to **30**, and then select **OK**.
13. Close the Group Policy Management Editor.

22.3.3 Task 3: Deploy LAPS client-side extension

1. Switch to **SEA-SVR1**, using **Contoso\Administrator** with the password **Pa55w.rd**.

   Note: You will be prompted to change your password, due to the previous exercise. Use the new password in place of the documented password throughout the remainder of the lab.

2. Enter the following command:

   ```
   Msiexec /I \\SEA-ADM1\c$\Labfiles\Mod08\LAPS.x64.msi
   ```

3. When the **Local Administrator Password Solution Setup Wizard** opens, select **Next**.
4. Select **I accept the terms in the License Agreement**, and then select **Next**.
5. Select **Next** again, and then select **Install**.
6. Select **Finish**.
7. Enter the following command:

   ```
   gpupdate /forces
   ```

22.3.4 Task 4: Verify LAPS

1. Switch to **SEA-ADM1**.
2. Select **Start**, select **LAPS**, and then select **LAPS UI**.
3. In the **LAPS UI** dialog box, in the **ComputerName** text box, enter **SEA-SVR1**, and then select **Search**.
4. Review the **Password** and the **Password expires** values, and then select **Exit**.
5. In the Windows PowerShell window, enter the following command:

   ```
   Get-ADComputer SEA-SVR1 -Properties ms-Mcs-AdmPwd
   ```

6. Review the password assigned to SEA-SVR1.
7. Close the gridview window.

22.4 lab: title: 'Lab: Implementing RDS in Windows Server' type: 'Answer Key' module: 'Module 9: RDS in Windows Server'

23 Lab answer key: Implementing RDS in Windows Server

23.0.1 Exercise 1: Implementing RDS

23.0.1.1 Task 1: Install RDS

23.0.1.1.1 Install RDS using Server Manager

1. On **SEA-RDS1**, select the **Start** button, and then select the **Server Manager** tile.
2. In **Server Manager**, select **Manage**, and then select **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, on the **Before you begin** page, select **Next**.
4. On the **Select installation type** page, select **Remote Desktop Services installation**, and then select **Next**.
5. On the **Select deployment type** page, verify that **Standard deployment** is selected, and then select **Next**.

   NOTE: Even though, we could have selected the **Quick Start** deployment option and have all three required Remote Desktop Services (RDS) role services installed on **SEA-RDS1**, you selected the **Standard deployment** option to practice selecting different servers for the RDS role services. Furthermore, the **Quick Start** deployment option will create a collection named **QuickSessionCollection** and publish the following RemoteApp Programs: **Calculator**, **Paint**, and **WordPad**.
6. On the **Select deployment scenario** page, select **Session-based desktop deployment**, and then select **Next**.
7. On the **Review role services** page, review the description of the role services, and then select **Next**.
8. On the **Specify RD Connection Broker server** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`. Add the computer to the **Selected** section by selecting the Right arrow, and then select **Next**.
9. On the **Specify RD Web Access server** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`. Add the computer to the **Selected** section by selecting the Right arrow, and then select **Next**.
10. On the **Specify RD Session Host servers** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`. Add the computers to the **Selected** section by selecting the Right arrow, and then select **Next**.
11. On the **Confirm selections** page, select **Cancel**

23.0.1.1.2 Install RDS using Windows PowerShell

NOTE: We will now do the actual installation of RDS using Windows PowerShell. The previous steps were included to demonstrate how to install RDS using Server Manager.

1. Switch to **SEA-DC1**. and
2. In the **Administrator: C:\Windows\system32\cmd.exe** command prompt window, enter the following command, and then select Enter: `powershell`
3. In the **Administrator: C:\Windows\system32\cmd.exe - powershell** window, enter the following command, and then select Enter: `$SVR="SEA-RDS1.contoso.com"`
4. In the **Administrator: C:\Windows\system32\cmd.exe - powershell** window, enter the following command, and then select Enter: `New-RDSessionDeployment -ConnectionBroker $SVR -WebAccessServer $SVR -SessionHost $SVR`
5. Wait for the installation to complete, which will take approximately 5 minutes, and then wait as **SEA-RDS1** restarts automatically.
6. Switch to **SEA-RDS1** and sign in as **Contoso\Administrator** with the password **Pa55w.rd**
7. Select the **Start** icon, and then select the **Server Manager** tile.
8. Wait for **Server Manager** to refresh.
9. In **Server Manager**, in the navigation pane, select **Remote Desktop Services**. You might need to select **Remote Desktop Services** twice.

23.0.1.2 Task 2: Create a Session Collection

23.0.1.2.1 Create and configure a Session Collection using Server Manager

NOTE: RDS in Windows Server supports two types of Session Collections on a single RD Session Host: an RD Session Collection, or a RemoteApp Session Collection. You cannot run both session collection types on the same RD Session Host by default. Therefore, when you're doing this exercise, you will first create an RD Session Host collection and verify that it works and then create a RemoteApp Session collection and verify that as well.

1. On **SEA-RDS1**, in **Server Manager**, on the **Remote Desktop Service Overview** page, select **Collections**.
2. In the details pane under **COLLECTIONS**, select **TASKS**, and then select **Create Session Collection**. You might need to scroll to the right to find this option.
3. In the **Create Collection Wizard**, on the **Before you begin** page, select **Next**.
4. On the **Name the collection** page, in the **Name** field, enter **IT**, and then select **Next**.
5. On the **Specify RD Session Host servers** page, in the **Server Pool** section, select `SEA-RDS1.Contoso.com`. Add the computers to the **Selected** section by selecting the Right arrow, and then select **Next**.
6. On the **Specify user groups** page, select **Remove** to remove **CONTOSO\Domain Users**, and then select **Add**.
7. In **the Enter the object names to select** field, enter **it**.
8. Select **Check Names**, and then select **OK**.
9. Verify that **CONTOSO\IT** is listed under **User Groups**, and then select **Next**.
10. On the **Specify user profile disks** page, clear the **Enable user profile disks** check box, and then select **Next**.
11. On the **Confirm selections** page, select **Cancel**, and when prompted, select **Yes**.
12. Minimize **Server Manager**.

23.0.1.2.2 Create and configure a session collection using Windows PowerShell

NOTE: We will now create and configure the session collection using Windows PowerShell. The previous steps were included to demonstrate how to create a session collection using Server Manager.

1. ON **SEA-RDS1**, right-click or access the context menu for the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `New-RDSessionCollection -CollectionName IT -SessionHost SEA-RDS1.Contoso.com -CollectionDescription "This Collection is for the IT department in Contoso" -ConnectionBroker SEA-RDS1.Contoso.com`
3. Wait for the command to complete, which will take approximately 1 minute.
4. Maximize **Server Manager**, and then select **Overview**.
5. Refresh **Server Manager** by selecting the F5 key.
6. In **Server Manager**, in the navigation pane, select **Collections**, and then verify that a collection named **IT** is listed in the details pane.

23.0.1.3 Task 3: Configure the Session Collection properties

23.0.1.3.1 Configure device redirection settings

1. On SEA-RDS1, in the navigation pane, select the **IT** collection.
2. Next to **PROPERTIES**, select **TASKS**., and then select **Edit Properties**.
3. On the **Session Collection** page, select the various settings and notice how the collection is configured.
4. Select **Client Settings**, and verify that both **Audio and video playback** and **Audio recording** is enabled.
5. Select **User Profile Disks**, and verify that **User Profiles Disks** is not enabled.
6. In the **IT Properties** dialog box, select **Cancel**.
7. Minimize **Server Manager**.
8. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `Get-RDSessionCollectionConfiguration -CollectionName IT -Client | Format-List`
9. Examine the output and notice that next to **ClientDeviceRedirectionOptions**, the following entries are listed:
   - **AudioVideoPlayBack**
   - **AudioRecording**

- **PlugAndPlayDevice**
- **SmartCard**
- **Clipboard**
- **LPTPort**
- **Drive**

10. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:`Set-RDSessionCollectionConfiguration -CollectionName IT -ClientDeviceRedirectionOptions PlugAndPlayDevice, SmartCard,Clipboard,LPTPort,Drive`
11. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:`Get-RDSessionCollectionConfiguration -CollectionName IT -Client | Format-List`
12. Examine the output, and notice that next to **ClientDeviceRedirectionOptions** only the following entries are listed now:
    - **PlugAndPlayDevice**
    - **SmartCard**
    - **Clipboard**
    - **LPTPort**
    - **Drive**

23.0.1.3.2 Configure User Profile Disks for IT collection

1. Switch to **SEA-DC1**.
2. In the **Administrator: C:\Windows\system32\cmd.exe - powershell** window, enter the following commands, one line at a time, and then select Enter:

- `New-Item C:\RDSUserProfiles -itemtype directory`
- `New-SMBShare -Name "RDSUserProfiles" -Path "C:\RDSUserProfiles" -FullAccess "Contoso\SEA-RDS1$", "Contoso\administrator"`
- `$acl = Get-Acl C:\RDSUserProfiles`
- `$AccessRule = New-Object System.Security.AccessControl.FileSystemAccessRule("Contoso\SEA-RDS1$","F`
- `$acl.SetAccessRule($AccessRule)`
- `$acl | Set-Acl C:\RDSUserProfiles`

2. Verify that each command executes successfully.
3. Switch to SEA-RDS1.
4. In the navigation pane, select the **IT** collection.
5. Next to **PROPERTIES**, select **TASKS**, and then select **Edit Properties**.
6. On the **Session Collection** page, select **User Profile Disks**, and then select **Enable user profile disks**.
7. In the **Location** field, enter **\\SEA-DC1\RDSUserProfiles**. In the **Maximum size (in GB)**, enter **10**, and then select **OK**.

23.0.1.4 Task 4: Connect to the Session Collection from RD Web portal

1. On **SEA-CL1**, on the taskbar, select the **Microsoft Edge** icon.
2. In **Microsoft Edge**, in the address bar, enter `https://SEA-RDS1.Contoso.com/rdweb`.
3. On the **This site is not secure** page, select **Details**, and then select **Go on to the webpage**.

   NOTE: This page opens because RD Web is using a self-signed certificate that is not trusted by the client. In a real production deployment, you would use trusted certificates.

4. On the **RD Web Access** page, in the **Domain\user name** field, enter **contoso\jane**. In the **Password** field, enter **Pa55w.rd**, and then select **Sign in**.
5. If prompted by **Microsoft Edge** to save the password, select **Never**.
6. On the **RD Web Access** page, under **Current folder: /**, select **IT**, and when prompted, select **Open**.
7. In the **Remote Desktop Connection** dialog box, select **Connect**.

   NOTE: This prompts the **Unknown publisher** pop up window because certificates for RDS have not yet been configured.

8. In the **Windows Security** dialog box, in the **Password** field, enter **Pa55w.rd**, then wait for the connection to complete.
9. In **SEA-RDS1**, right-click or access the context menu for **Start**, select **Shut down or sign out**. and then select **sign-out**.
10. Back on the **RD Web Access** page, select **Sign out**.

11. Close **Microsoft Edge**.

23.0.1.4.1 Verify User Profile Disk creation

1. Switch to **SEA-DC1**, and in the **Administrator: C:\Windows\system32\cmd.exe - powershell** window, enter the following command, and then select Enter: `cd\`
2. Enter the following command, and then select Enter: `cd RDSUserProfiles`
3. Enter the following command, and then select Enter: `dir`
4. Examine the contents of the **RDSUserProfiles** folder. Verify that there is a **.vhdx** file with an SID (a long string that starts with **S-1-5-21**) in its name.

23.0.2 Exercise 2: Configuring RemoteApp collection settings

23.0.2.1 Task 1: Create and configure a RemoteApp collection using Server Manager

1. Switch to **SEA-RDS1**.
2. Maximize **Server Manager**, and in the details pane. next to **REMOTEAPP PROGRAMS**, select **TASKS**, then select **Publish RemoteApp Programs**.
3. On the **Select RemoteApp programs** page, scroll down in the list under **The RemoteApp programs are populated from** `SEA-RDS1.CONTOSO.COM`. Select **WordPad** and select **Next**.
4. On the **Confirmation** page, select **Publish**, and wait for the RemoteApp to be published.
5. On the **Completion** page, verify that **WordPad** is listed in the details pane under **RemoteApp Program**, and then select **Close**.

23.0.2.2 Task 2: Create and configure a RemoteApp program using Windows PowerShell

1. ON **SEA-RDS1**, right-click or access the context menu for **Start**, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `New-RDRemoteApp -Alias Paint -DisplayName Paint -FilePath "C:\Windows\system32\mspaint.exe" -ShowInWebAccess 1 -collectionname IT -ConnectionBroker SEA-RDS1.Contoso.com`
3. When the command has completed, review the information about the published app, and then minimize the WindowsPowerShell window.
4. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `Get-RDRemoteApp -CollectionName IT`
5. Examine the output of the command. Notice that you will get a list of all published RemoteApp programs.
6. Maximize **Server Manager**, and then select **Overview**.
7. Refresh **Server Manager** by selecting F5.
8. In **Server Manager**, in the navigation pane, select the **IT** collection and verify that **Paint** is listed in the details pane under **REMOTEAPP PROGRAMS**.

23.0.2.3 Task 3: Run RemoteApp from RD Web portal

1. On **SEA-CL1**, on the taskbar, select the **Microsoft Edge** icon. In **Microsoft Edge**, in the address bar, enter `https://SEA-RDS1.Contoso.com/rdweb`, and then select Enter.
2. On the **This site is not secure page**, select **Details**, and then select **Go on to the webpage**.

   NOTE: This page opens because RD Web is using a self-signed certificate that is not trusted by the client. In a real production deployment, you would use trusted certificates.

3. On the **RD Web Access** page, in the **Domain\user name** field, enter **contoso\jane**. In the **Password** field, enter **Pa55w.rd**, and then select **Sign in**. If prompted by **Microsoft Edge** to save the password, select **Never**.
4. On the **RD Web Access** page, under **Current folder: /**, select **Paint**, and when prompted, select **Open**.
5. In the **Remote Desktop Connection** dialog box, select **Connect**.

   NOTE: The **Unknown publisher** pop-up window displays because you have not yet configured certificates for RDS.

6. In the **Windows Security** dialog box, in the **Password** field, enter **Pa55w.rd**.
7. Wait for the RemoteApp **Paint** program to start, and then test its functionality.
8. In **Paint**, select **File**, and then select **Exit** to close the application.
9. Back on the **RD Web Access** page, select **Sign out**.
10. Close Microsoft Edge.

23.0.3 Exercise 3: Configure a virtual desktop template

23.0.3.1 Task 1: Verify the operating system (OS) version

1. On **SEA-CL1**, sign in as **.\Admin** with the password **Pa55w.rd**.
2. Select the Start button, enter **pc**, and then select **About your pc**.
3. In the **Settings** app, on the **About screen**, verify the following information:
   - The Windows operating system edition is Windows 10 Enterprise
   - The System type is 64-bit OS
4. Close the **Settings** app.

23.0.3.2 Task 2: Disable unnecessary services

1. On **SEA-CL1**, select the **Start** button, and enter **services**, and then select **Services**.
2. In the **Services** window, right-click or access the context menu for **Background Intelligent Transfer Service**.
3. In the **Background Intelligent Transfer Service Properties (Local Computer)** dialog box, on the **General** tab, select **Stop**.
4. In the **Startup type** box, select **Disabled**, and then select **OK**.
5. In the **Services** window, right-click or access the context menu for **Diagnostic Policy Service**.
6. In the **Diagnostic Policy Service Properties (Local Computer)** dialog box, on the **General tab**, select **Stop**.
7. In the **Startup type** box, select **Disabled**, and then select **OK**.
8. In the **Services** window, right-click or access the context menu for **Shell Hardware Detection**.
9. In the **Shell Hardware Detection Properties (Local Computer)** dialog box, on the **General** tab, select **Stop**.
10. In the **Startup type** box, select **Disabled**, and then select **OK**.
11. In the **Services** window, right-click or access the context menu for **Volume Shadow Copy**.
12. In the **Volume Shadow Copy Properties (Local Computer** dialog box, on the **General** tab, select **Stop**.
13. In the **Startup type** box, select **Disabled**, and then select **OK**.
14. In the **Services window**, right-click or access the context menu for **Windows Search**.
15. In the **Windows Search Properties (Local Computer)** dialog box, on the **General** tab, select **Stop**.
16. In the **Startup type** box, select **Disabled**, and then select **OK**.
17. In the **Services** window, select **File**, and then select **Exit**.

23.0.3.3 Task 3: Disable unnecessary scheduled tasks

1. On **SEA-CL1**, select the **Start** button, enter **sch**, and then select **Task Scheduler**.
2. In the **Task Scheduler** window, expand **Task Scheduler Library**, expand **Microsoft**, expand **Windows**, and then select **Defrag**.
3. Right-click or access the context menu for **ScheduledDefrag**, and then select **Disable**.
4. In the **Task Scheduler** window, select **File**, and then select **Exit**.

23.0.3.4 Task 4: Prepare the virtual desktop template by using Sysprep

1. On **SEA-CL1**, open **File Explorer**. Browse to **C:\Windows\System32\Sysprep**, right-click or access the context menu for **sysprep.exe**, and then select **Open**.
2. In the **System Preparation tool 3.14** dialog box, in the **System Cleanup Action** box, select **Enter System Out-of-Box Experience (OOBE)**.
3. Select the **Generalize** check box.
4. In the **Shutdown Options** box, select **Shutdown**, and then select **OK**.
5. Wait while the System Preparation Tool (Sysprep) completes and shuts down the VM.

23.1 Results: After completing this exercise, you will have prepared a Hyper-V VM to be a virtual desktop template.

23.2 lab: title: 'Lab: Deploying network workloads' type: 'Answer Key' module: 'Module 10: Remote Access and web services in Windows Server'

24 Lab answer key: Deploying network workloads

24.1 Lab setup

For this demonstration, you will use the following virtual machines:

- **WS-011T00A-SEA-DC1**
- **WS-011T00A-SEA-ADM1**
- **WS-011T00A-SEA-SVR1**
- **WS-011T00A-SEA-SVR3**
- **WS-011T00A-SEA-CL1**

Sign in by using the following credentials:

- User Name: **Contoso\Administrator**
- Password: **Pa55w.rd**

  Tip: You don't need to sign in to **WS-011T00A-SEA-DC1** as you don't use this machine in this lab.

24.2 Exercise 1: Implementing Web Application Proxy

24.2.1 Task 1: Install AD FS on SEA-DC1

1. On **SEA-SVR1**, enter **powershell.exe**, and then select Enter.
2. At the Windows PowerShell prompt, enter `C:\Labfiles\Mod03\InstallADFS.ps1`, and then select Enter.
3. Wait for the restarting message to display.

24.2.2 Task 2: Create DNS entries for AD FS and Web Application Proxy

1. On **SEA-ADM1**, on the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, select **Windows Admin Center**.
3. In the **Windows Security** dialog box, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
4. In **Windows Admin Center**, select **SEA-DC1**.
5. In the **Specify your credentials** dialog box, select **Use another account for this connection**, and then sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
6. On the **Tools** pane, select **DNS**, and then on the right **details** pane, select **Install**.
7. When the DNS PowerShell tools installation is complete, select `Contoso.com`, and then select **Create new DNS record**.
8. In the **Create a new DNS record** dialog box, enter the following information, and then select **Create**:
   - DNS record type: **Host (A)**
   - Record name: **remoteapp**
   - IP address: **172.16.10.14**
   - Time to live: **3600**
9. Select **Create a new DNS record**, enter the following information, and then select **Create**:
   - DNS record type: **Host (A)**
   - Record name: **fs**
   - IP address: **172.16.10.12**
   - Time to live: **3600**

24.2.3 Task 3: Install Remote Access management tools

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Windows Admin Center**, and then select `sea-adm1.contoso.com [gateway]`.
2. On the **Tools** pane, select **Roles & features**.

3. On the **Roles and features** pane, under **Features**, expand **Remote Server Administration Tools**, expand **Role Administration Tools**, select the **Remote Access Management Tools** check box, and then select **Install**.
4. In the **Install Roles and Features** dialog box, select **Yes**.

24.2.4 Task 4: Install Web Application Proxy

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Windows Admin Center**, and then select **SEA-SVR3**.
2. In the **Specify your credentials** dialog box, select **Use another account for this connection**, and then sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
3. On the **Tools** pane, select **Roles & features**.
4. On the **Roles and features** pane, expand **Remote Access**, select the **Web Application Proxy** check box, and then select **Install**.
5. In the **Install Roles and Features** dialog box, select **Yes**.

24.2.5 Task 5: Configure Web Application Proxy

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Tools**, and then select **Remote Access Management**.
3. In the **Remote Access Management Console**, on the **Tasks** pane, select **Manage a Remote Server**.
4. In the **Manage a Remote Server** dialog box, enter **SEA-SVR3**, and then select **OK**.
5. In the **Remote Access Management Console**, select **Web Application Proxy**, and then select **Run the Web Application Proxy Configuration Wizard**.
6. In the **Web Application Proxy Configuration Wizard**, select **Next**.
7. On the **Federation Server** screen, enter the following information, and then select **Next**:
   - Federation service name: `fs.Contoso.com`
   - User name: **Contoso\Administrator**
   - Password: **Pa55w.rd**
8. On the **AD FS Proxy Certificate** screen, in the **Select a certificate to be used by the AD FS proxy** box, select `fs.contoso.com`, and then select **Next**.
9. On the **Confirmation** screen, read the information, and then select **Configure**.
10. On the **Results** screen, select **Close**.

    Note: If you get an error in **Remote Access Management Console** indicating that cmdlets are not found, restart **Remote Access Management Console**.

24.2.6 Task 6: Configure a web application

1. On **SEA-ADM1**, in the **Remote Access Management Console**, in the **Tasks** pane, select **Publish**.
2. In the **Publish New Application Wizard**, on the **Welcome** screen, select **Next**.
3. On the **Preauthentication** screen, select **Pass-through**, and then select **Next**.
4. On the **Publishing Settings** screen, enter the following information, and then select **Next**.
   - Name: **RemoteApp**
   - External URL: `https://remoteapp.contoso.com`
   - External certificate: `remoteapp.contoso.com`
   - Backend server URL: `https://SEA-ADM1.contoso.com`

     Note: You will receive a warning that external URL and backend URL are different. You can ignore this warning.
5. On the **Confirmation** screen, select **Publish**.
6. On the **Results** screen, select **Close**.

24.2.7 Task 7: Configure Windows Defender Firewall to allow remote access

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Windows Admin Center**, and then select `sea-adm1.contoso.com[gateway]`.
2. In the **Tools** pane, select **Firewall**.
3. In the **Firewall** pane, select **Incoming rules**, and then select **New**.
4. In the **New Rule** dialog box, enter the following information, and then select **Create**:

- Name: **SecureWeb**
- Direction: **Incoming**
- Action: **Allowed**
- Enable firewall rule: **Yes**
- Protocol: **TCP**
- Local port: **443**
- Remote port: **blank**
- ICMP types: **blank**
- Profiles: **Select All**

24.2.8 Task 8: Test the web application

1. On **SEA-CL1**, on the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, in the address bar, enter `https://remoteapp.contoso.com`, and then select Enter.
3. In the **Windows Security** dialog box, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.

24.2.9 Exercise 2: Implementing VPN in Windows Server

24.2.9.1 Task 1: Configure RRAS service and NPS policies for VPN

1. On **SEA-ADM1**, right-select (or access the context menu) the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `Install-WindowsFeature -name RemoteAccess,Routing -IncludeManagementTools`
3. Wait for the command to complete, which should take approximately 1 minute.
4. Leave the **Administrator: Windows PowerShell** window open.

24.2.9.1.1 Request certificate for SEA-ADM1

1. On SEA-ADM1, in the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `mmc`
2. In the **Console** window, select **File**, and then select **Add/Remove Snap-in**.
3. In the **Available snap-ins** list, select **Certificates**, and then select **Add**.
4. In the **Certificates snap-in** dialog box, select **Computer account**, and then select **Next**.
5. In the **Select Computer** dialog box, verify that **Local computer** is selected, select **Finish**, and then select **OK**.
6. In the **Certificates** snap-in, in the console tree of the **Certificates** snap-in, navigate to **Certificates (Local Computer)\Personal**.
7. Right-click (or access the context menu) **Personal**, point to **All Tasks**, and then **select Request New Certificate**.
8. On the **Before you begin** page, select **Next**, and then on the **Select Certificate Enrollment Policy** page, select **Next**.
9. On the **Request Certificates** page, select **Contoso Web Server**, and then select the **More information is required to enroll for this certificate. Click here to configure settings** link.
10. In the **Certificate Properties** dialog box, on the **Subject** tab, under **Subject name**, under **Type**, select **Common name**.
11. In the **Value** text box, enter `vpn.contoso.com`, and then select **Add**.
12. Select the **General** tab, and in the **Friendly name** field, enter **Contoso VPN**.
13. Select **OK**, select **Enroll**, and then select **Finish**.
14. In the **Certificates** snap-in, expand **Personal** and then select **Certificates**.
15. In the **details** pane, verify that a new certificate with the name `vpn.contoso.com` is enrolled with **Intended Purposes** of **Server Authentication**.
16. In the **Microsoft Management Console (MMC)**, select **File**, and then select **Exit**. When you receive a prompt to save the settings, select **No**.

24.2.9.1.2 Change the HTTPS bindings

1. On **SEA-ADM1**, open **Server Manager**, select **Tools**, and then select **Internet Information Services (IIS) Manager.**
2. In the **Internet Information Services (IIS) Manager**, expand **SEA-ADM1 (CONTOSO\Administrator)**.
3. In the **Internet Information Services (IIS) Manager**, in the console tree, expand **Sites**, and then select **Default Web site**.

4. In the **Actions** pane, select **Bindings**, and then select **Add**.
5. In the **Add Site Binding** dialog box, under the **Type** select **https**, in the SSL Certificate list, select the **Contoso VPN** certificate, select **OK**, select **Yes** when prompted, and then select **Close**.
6. Close the **Internet Information Services (IIS) Manager** console.

24.2.9.1.3 Configure and enable VPN configuration

1. On **SEA-ADM1**, in the **Server Manager**, select **Tools**, and then select **Routing and Remote Access**.
2. Right-click (or access the context menu) **SEA-ADM1 (local)**, and then select **Configure and Enable Routing and Remote Access**.
3. On the **Welcome to Routing and Remote Access Server Setup Wizard**, select **Next**.
4. On the **Configuration** page, select **Custom configuration**, and then select **Next**.
5. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then select **Next**.
6. On the **Completing the Routing and Remote Access Server Setup Wizard** page, select **Finish**.
7. When you receive a prompt, select the **Routing and Remote Access** dialog box, and then select **Start service**.
8. Expand **SEA-ADM1 (local)**, right-click (or access the context menu) **Ports**, and then select **Properties**.
9. In the **Ports Properties** dialog box, verify that 128 ports exist for **WAN Miniport (SSTP)**, **WAN Miniport (IKEv2)**, **WAN Miniport (L2TP)**, and **WAN Miniport (PPTP)**.
10. Select **WAN Miniport (SSTP)** and select **Configure**. In the **Maximum ports** text box, enter **5**, and then select **OK**.
11. In the **Routing and Remote Access** message box, select **Yes**.
12. Repeat steps 10 and 11 for IKEv2 and L2TP.
13. Select **WAN Miniport (PPTP)** and select **Configure**. In the **Configure Device - WAN Miniport (PPTP)** windows, remove the check mark next to **Remote access connections (inbound only)** and **Demand-dial routing connections (Inbound and outbound)**, and then select **OK**.
14. To close the **Ports Properties** dialog box, select **OK**.
15. Right-click (or access the context menu) **SEA-ADM1 (local)**, and then select **Properties**.
16. In the **SEA-ADM1 (local) Properties** dialog box, on the **General** tab, verify that **IPv4 Remote access server** is selected.
17. Select the **Security** tab, and then select **Authentication Methods**. Verify that **Extensible authentication protocol (EAP)** is selected as the authentication protocol, and then select **OK**.
18. On the **Security** tab, select the drop-down arrow next to **Certificate**, and then select `vpn.contoso.com`.
19. Select the **IPv4** tab, and then verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
20. To close the **SEA-ADM1 (local) Properties** dialog box, select **OK** and then select **Yes** when prompted.

24.2.9.1.4 Configure the Remote Access policies on NPS

1. On **SEA-ADM1**, in **Server Manager**, on the **Tools** menu, select **Network Policy Server**.
2. In the **Network Policy Server** console, in the **navigation** pane, expand **Policies**, and then select **Network Policies**.
3. In the **navigation** pane, right-click (or access the context menu) **Network Policies**, and then select **New**.
4. In the **New Network Policy** Wizard, in the **Policy name** text box, enter **Contoso IT VPN**.
5. In the **Type of network access server** list, select **Remote Access Server(VPN-Dial up)**, and then select **Next**.
6. On the **Specify Conditions** page, select **Add**.
7. In the **Select condition** dialog box, select **Windows Groups**, and then select **Add**.
8. In the **Windows Groups** dialog box, select **Add Groups**.
9. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** text box, enter **IT**, select **Check Names**, and then select **OK** select **OK** again, and then select **Next**.
10. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then select **Next**.
11. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
12. To add **EAP Types**, select **Add**.
13. On the **Add EAP** page, select **Microsoft Secured password (EAP-MSCHAP v2)**, and then select **OK**.
14. To add **EAP** types, select **Add**.
15. On the **Add EAP** page, select **Microsoft: Smart Card or other certificate**, select **OK**, and then

select **Next**.
16. On the **Configure Constraints** page, select **Next**.
17. On the **Configure Settings** page, select **Next**.
18. On the **Completing New Network Policy** page, select **Finish**.
19. Close all open windows.

24.2.9.2 Task 2: Configure a client VPN connection

1. On **SEA-CL1**, right-click (or access the context menu) the **Start** button, and then select **Network Connections**.
2. In **Network & Internet**, select **VPN**, and then select **Add a VPN connection**.
3. In the **Add a VPN connection** wizard, configure the following settings, and then select **Save**:
   - VPN provider: **Windows (built-in)**
   - Connection name: **Contoso VPN**
   - Server name or address: `vpn.contoso.com`
   - VPN type: **Secure Socket Tunneling Protocol (SSTP)**
   - Type of sign-in info: **User name and password**
   - Remember my sign-in info: **Cleared**. You might need to scroll down to find this setting.

24.2.9.3 Task 3: Test the VPN connection

1. Still in **Network & Internet**, select **Contoso VPN**, and then select **Connect**.
2. In the **Sign in** dialog box, in the **User name** text box, enter **contoso\jane**, in the **Password text** box, enter **Pa55w.rd**, and then select **OK**.
3. Verify that **Connected** displays under **Contoso VPN**, indicating that you are now connected to the VPN server.
4. In **Network & Internet**, select **Ethernet** and then under **Related settings**, select **Network and Sharing Center**.
5. In **Network and Sharing Center**, select **Change Adapter settings**.
6. Verify that **WAN Miniport (SSTP)** displays under **Contoso VPN**.

24.2.9.4 Verify connection on client and VPN server

1. On **SEA-CL1**, right-click (or access the context menu) the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `Get-NetIPConfiguration`
3. Examine the output and verify that **Contoso VPN** is listed next to **InterfaceAlias**. Also verify that the **Contoso VPN** interface has been issued an IP Address. This is the IP address for VPN connection assigned by RRAS.
4. Switch to **SEA-ADM1** and maximize the **Routing and Remote Access** snap-in.
5. In the **Routing and Remote Access** snap-in, select **Remote Access Clients (0)** and verify that **Contoso\jane** is listed under the **User Name** column. This indicates that the user is connected to the VPN Server.
6. Maximize **Server Manager**, select the **Tools** menu, and then select **Remote Access Management**.
7. In the **Remote Access Management** console, select **Remote Client Status** and verify that **CONTOSO\jane** is listed in the **details** pane under **Connected Clients**. Notice that the VPN protocol displays under the **Protocol/Tunnel** field as **Sstp**.

Question: Why did you disable the PPTP authentication protocol when you configured the ports of the VPN Server?

Answer: The PPTP protocol is considered highly insecure and you shouldn't use it.

Results: After completing this exercise, you should have installed and configured the Remote Access server to successfully provide VPN access.

24.2.10 Exercise 3: Deploying and configuring web server

24.2.10.1 Task 1: Install the Web Server role

1. On **SEA-SVR1**, in the **Administrator C:\Windows\system32\cmd.exe** window, enter the following command, and then select Enter: `powershell`

2. In the **Administrator C:\Windows\system32\cmd.exe - powershell** window, enter the following command, and then select Enter: `Install-WindowsFeature -name Web-Server -IncludeManagementTools`
3. Wait for the command to complete, which should take approximately one minute.
4. Verify that **True** displays under **Success** in the output.

24.2.10.1.1 Verify the Web Server installation

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, if not already open.
2. In the Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-eventLog System -After (Get-Date).AddHours(-1)` Verify that no errors display under the **EntryType** column.
3. Still in the Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-eventLog Application -After (Get-Date).AddHours(-1)` Verify that only errors with word **License** display under the **Message** column.

24.2.10.1.2 Verify that the Windows Firewall rules for HTTP and HTTPS traffic are enabled

1. On **SEA-SVR1**, in a Windows PowerShell command prompt, enter the following command, and then select Enter:`Get-NetFirewallProfile -Name Domain | Get-NetFirewallRule | where-Object {$_.DisplayName -like "World Wide Web*"}`
2. This will return information about two rules. One for HTTP and one for HTTPS. Verify that both rules are enabled and allow inbound traffic.
3. Examine the **Enabled** value. It should display **True**. Also examine the **Direction** value, which should display **Inbound**.
4. Leave the Windows PowerShell command prompt open.

24.2.10.1.3 Test the default website

1. Switch to **SEA-ADM1** and in the taskbar select the Microsoft edge icon, which is to the right of the **File Explorer** icon.
2. In Microsoft Edge, enter **`http://SEA-SVR1`** in the address bar, and then select Enter.
3. Verify that IIS displays the default, **Internet Information Services** webpage.
4. In Microsoft Edge, enter **`http://172.16.10.12`** in the address bar, and then select Enter.
5. Verify that IIS displays the default, **Internet Information Services webpage**.
6. Leave Microsoft Edge open.

24.2.10.2 Task 2: Configure Web Server options

24.2.10.2.1 Configure DNS for the default website

1. On **SEA-ADM1**, right-click (or access the context menu) the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: `Add-DnsServerResourceRecordA -ComputerName SEA-DC1 -Name "www" -ZoneName "contoso.com" -AllowUpdateAny -IPv4Address "172.16.10.12"`
3. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter:`Get-DnsServerResourceRecord -ComputerName SEA-DC1 -ZoneName "contoso.com"`
4. In the output, verify **www** displays in the **HostName** column and that **172.16.10.12** displays under the **RecordData** column in the same row as the **www** entry.

24.2.10.2.2 Test the website by using DNS names

1. In Microsoft Edge, enter **`http://www.contoso.com`** in the address bar, and then select Enter.
2. Verify that IIS displays the default, **Internet Information Services webpage**.

24.2.10.2.3 Enable remote management of IIS using IIS Manager

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, if it's not already open.
2. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter: `Install-WindowsFeature -Name Web-Mgmt-Service` Wait for the command to complete, which should take approximately one minute.

3. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:`Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\WebManagement\Server' -Name EnableRemoteManagement -Value 1`
4. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:`Restart-Service wmsvc`

   Note: Setting this registry key to 1 will enable remote management of IIS. You must restart the **Web Management Service (wmsvc)** after changing the registry key.

5. On **SEA-ADM1**, open a Windows PowerShell command prompt, if it's not already open.
6. On **SEA-ADM1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:`Install-WindowsFeature -Name Web-Mgmt-Console,Web-Scripting-Tools`. Wait for the command to complete, which should take approximately one minute.

   Note: The output from this command will return **NoChangeNeeded** under the **Exit Code** column. This is because, you already installed the management tools during exercise 1. This step has been left here intentionally to show the complete process of enabling remote management of IIS.

7. On **SEA-ADM1**, select the **Start** button, and then select the **Server Manager** tile. In **Server Manager**, select **Tools**, and then select **Internet Information Services (IIS) Manager**.
8. On the **Start Page**, under **Connection tasks**, select **Connect to a server**. Use the following information and select **Finish** to complete the wizard:
   - Server name: **SEA-SVR1**
   - User name: **contoso\administrator**
   - Password: **Pa55w.rd**
   - When prompted by the **Server Certificate Alert** dialog window, select **Connect**
   - Connection name: **SEA-SVR1**
9. In the **Connections** pane, select **Start Page**. **Notice Recent connections**, **Connection tasks**, **Online resources**, and **IIS News**.
10. In the **Connections** pane, select **SEA-SVR1 (contoso\administrator)**. Notice the icons listed in the **Features View** pane. In the **Actions** pane, notice the list of **Manage Server** actions.
11. In the **Connections** pane, expand **SEA-SVR1 (contoso\administrator)**, and then select **Sites**. In the **Features View** pane, notice the **Name** of the listed website and its **Status**.
12. In the **Actions** pane, select **Set Website Defaults**. In the **Website Defaults** dialog box, notice the **Application Pool** setting. Select **Cancel**.
13. Leave **Internet Information Services (IIS) Manager** open.

24.2.10.3 Task 3: Create and configure a new site

24.2.10.3.1 Create a webpage in the default website

1. Switch to **SEA-SVR1**, and in the **Administrator C:\Windows\system32\cmd.exe - powershell** window, enter the following command, and then select Enter: `notepad`
2. In **Notepad**, enter the following:** Contoso intranet running on SEA-SVR1 **
3. In the menu bar, select **File**, and then select **Save As**. In the **Save As** dialog box, select **File name**, and then delete ***.txt**. In the **File name** box, enter **c:\inetpub\wwwroot\default.htm**.
4. In the **Text Documents (*.txt)** drop-down box, select **All Files**. Then select **Save**. Close **Notepad**.

24.2.10.3.2 Request a new Web Server certificate

1. On **SEA-SVR1**, in the **Administrator C:\Windows\system32\cmd.exe - powershell** window, enter the following command, and then select Enter:`Get-Certificate -Template ContosoWebServer -DnsName www.contoso.com -CertStoreLocation cert:\LocalMachine\My`.
2. Wait for the command to complete, which should take approximately 30 seconds.
3. In the output, verify that **Issued** displays under **Status**.

24.2.10.4 Task 4: Verify site functionality

1. Switch to **SEA-ADM1**, and in the **Internet Information Services (IIS) Manager**, right-click (or access the context menu) **Default Web Site** and select **Edit Bindings**.
2. In the **Site Bindings** dialog box, select **Add** and under **type**, select **https**.
3. Under **SSL certificate**, select the certificate displayed with a GUID, select **OK** and then select **Close**. The GUID will be similar to: **35B56A0F8D0AC682579BA893524EDFC6EC8FBA83**.
4. In Microsoft Edge, enter `http://www.contoso.com` in the address bar, and then select Enter.

5. Verify that IIS displays the default **Internet Information Services webpage**. Notice that **Not secure** displays next to `www.contoso.com`.
6. In the address bar, enter `https://www.contoso.com`. Verify that IIS displays the website. Notice that a padlock displays next to `www.contoso.com`. This means that the website is protected using SSL.

24.3 lab: title: 'Lab: Monitoring and troubleshooting Windows Server' type: 'Answer Key' module: 'Module 11: Monitoring, performance, and troubleshooting'

25 Lab answer key: Monitoring and troubleshooting Windows Server

25.0.1 Exercise 1: Establishing a performance baseline

Note: After starting the Data Collector Set, there might be a delay of 10 minutes for the results to appear.

25.0.1.1 Task 1: Create and start a data collector set

1. Switch to **SEA-ADM1**.
2. Select **Start**.
3. In the search box, enter **Perf**, and then in the **Best match** list, select **Performance Monitor**.
4. In **Performance Monitor**, expand **Data Collector Sets** in the navigation pane, and then select **User Defined**.
5. Right-click or access the context menu for **User Defined**, select **New**, and then select **Data Collector Set**.
6. In the **Create new Data Collector Set Wizard**, enter **SEA-ADM1 Performance** in the **Name** box.
7. Select **Create manually (Advanced)**, and then select **Next**.
8. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then select **Next**.
9. On the **Which performance counters would you like to log?** page, select **Add**.
10. In the **Available counters** list, expand **Processor**, select **% Processor Time**, and then select **Add**.
11. In the **Available counters** list, expand **Memory**, select **Pages/sec**, and then select **Add**.
12. In the **Available counters** list, expand **PhysicalDisk**, select **% Disk Time**, and then select **Add**.
13. Select **Avg. Disk Queue Length**, and then select **Add**.
14. In the **Available counters** list, expand **System**, select **Processor Queue Length**, and then select **Add**.
15. In the **Available counters** list, expand **Network Interface**, select **Bytes Total/sec**, select **Add**, and then select **OK**.
16. On the **Which performance counters would you like to log?** page, enter **1** in the **Sample interval** box, and then select **Next**.
17. On the **Where would you like the data to be saved?** page, select **Next**.
18. On the **Create the data collector set?** page, select **Save** and **close**, and then select **Finish**.
19. In **Performance Monitor**, in the results pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Start**.

25.0.1.2 Task 2: Create a typical workload on the server

1. Select **Start**, enter **Cmd** in the search box, and then select **Command Prompt** in the **Best match** list.
2. At the command prompt, enter the following command, and then select Enter:

   ```
   Fsutil file createnew bigfile 104857600
   ```

3. At the command prompt, enter the following command, and then select Enter:

   ```
   Copy bigfile \\SEA-dc1\c$
   ```

4. At the command prompt, enter the following command, and then select Enter:

```
Copy \\SEA-dc1\c$\bigfile bigfile2
```

5. At the command prompt, enter the following command, and then select Enter:

```
Del bigfile*.*
```

6. At the command prompt, enter the following command, and then select Enter:

```
Del \\SEA-dc1\c$\bigfile*.*
```

7. Don't close the **Command Prompt** window.

25.0.1.3 Task 3: Analyze the collected data

1. Switch to **Performance Monitor**.
2. In the navigation pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Stop**.
3. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **SEA-ADM1 Performance**, select **SEA-ADM1_DateTime-000001**, and then review the report data.
4. On the menu bar, select **Change graph type** or press Ctrl+G, and then select **Report**.
5. Record the values that are listed in the report for later analysis. Recorded values include:
   - **Memory\Pages/sec**
   - **Network Interface\Bytes Total/sec**
   - **PhysicalDisk% Disk Time**
   - **PhysicalDisk\Avg. Disk Queue Length**
   - **Processor% Processor Time**
   - **System\Processor Queue Length**

25.0.2 Results

After this exercise, you should have established a baseline for performance-comparison purposes.

25.0.3 Exercise 2: Identifying the source of a performance problem

25.0.3.1 Task 1: Create additional workload on the server

1. On **SEA-ADM1**, open File Explorer.
2. Browse to **C:\Labfiles\Mod11**.
3. Double-click or select **CPUSTRES64.EXE**, and then select Enter.
4. In the **CPU Stress - Sysinternals:www.sysinternals.com** dialog box, right-click or access the context menu for the highlighted thread at the top of the list of running threads, select **Activity Level**, and then select **Busy (75%)**.

25.0.3.2 Task 2: Capture performance data by using a data collector set

1. Switch to **Performance Monitor**.
2. In **Performance Monitor**, expand **Data Collector Sets**, and select **User Defined**.
3. In the results pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Start**.
4. Wait a minute to allow the data capture to occur.

25.0.3.3 Task 3: Remove the workload, and then review the performance data

1. After a minute, close CPUSTRES64 and File Explorer.
2. Switch to **Performance Monitor**.
3. In the navigation pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Stop**.
4. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **SEA-ADM1 Performance**, select **SEA-ADM1_DateTime-000002**, and then review the report data.
5. On the menu bar, select **Change graph type** or press Ctrl+G, and then select **Report**.
6. Record the following values:
   - **Memory\Pages/sec**
   - **Network Interface\Bytes Total/sec**

- **PhysicalDisk% Disk Time**
- **PhysicalDisk\Avg. Disk Queue Length**
- **Processor% Processor Time**
- **System\Processor Queue Length**

Question: Compared with your previous report, which values have changed?

Answer: Memory and disk activity are reduced, but processor activity has increased significantly.

Question: What would you recommend?

Answer: You should continue to monitor the server to ensure that the processor workload doesn't reach capacity.

25.0.4 Results

After this exercise, you should have used performance tools to identify a potential performance bottleneck.

25.0.5 Exercise 3: Viewing and configuring centralized event logs

25.0.5.1 Task 1: Configure subscription prerequisites

1. On **SEA-ADM1**, switch to the command prompt.
2. At the command prompt, enter the following command, and then select Enter:

   ```
   winrm quickconfig
   ```

3. You can observe that the WinRM service is already running and that it's set up for remote management.
4. On the taskbar, select **Server Manager**.
5. In **Server Manager**, select **Tools** on the toolbar, and then select **Computer Management**.
6. In **Computer Management (Local)**, expand **System Tools**, expand **Local Users and Groups**, and then select **Groups**.
7. In the results pane, double-click or select **Event Log Readers**, and then select Enter.
8. Select **Add**, and then in the **Select Users, Computers, Service Accounts or Groups** dialog box, select **Object Types**.
9. In the **Object Types** dialog box, select the **Computers** check box, and then select **OK**.
10. In the **Select Users, Computers, Service Accounts or Groups** dialog box, enter **SEA-CL1** in the **Enter the object names to select** box, and then select **OK**.
11. In the **Event Log Readers Properties** dialog box, select **OK**.
12. Switch to **SEA-CL1**.
13. Open a **Command Prompt** window, enter the following command at the command prompt, and then select Enter:

    ```
    Wecutil qc
    ```

14. Enter **Y** when prompted, and then select Enter.

25.0.5.2 Task 2: Create a subscription

1. Select **Start**, and then enter **Event** on the **Start** page.
2. In the **Best match** list, select **Event Viewer**.
3. In **Event Viewer**, select **Subscriptions** in the navigation pane.
4. Right-click or access the context menu for **Subscriptions**, and then select **Create Subscription**.
5. In the **Subscription Properties** dialog box, enter **SEA-ADM1 Events** in the **Subscription name** box.
6. Select **Collector initiated**, and then select **Select Computers**.
7. In the **Computers** dialog box, select **Add Domain Computers**.
8. In the **Select Computer** dialog box, enter **SEA-ADM1** in the **Enter the object name to select** box, and then select **OK**.
9. In the **Computers** dialog box, select **OK**.
10. In the **Subscription Properties – SEA-ADM1 Events** dialog box, select **Select Events**.

11. In the **Query Filter** dialog box, select the **Critical**, **Warning**, **Information**, **Verbose**, and **Error** check boxes.
12. In the **Logged** drop-down list, select **Last 7 days**.
13. In the **Event logs** drop-down list, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **Diagnosis-PLA**, and then select the **Operational** check box.
14. In the **Query Filter** dialog box, select **OK**.
15. In the **Subscription Properties – SEA-ADM1 Events** dialog box, select **OK**.

25.0.5.3 Task 3: Configure a performance counter alert

1. Switch to **SEA-ADM1**.
2. In **Performance Monitor**, expand **Data Collector Sets** in the navigation pane, and then select **User Defined**.
3. Right-click or access the context menu for **User Defined**, select **New**, and then select **Data Collector Set**.
4. In the **Create new Data Collector Set Wizard**, enter **SEA-ADM1 Alert** in the **Name** box.
5. Select **Create manually (Advanced)**, and then select **Next**.
6. On the **What type of data do you want to include?** page, select **Performance Counter Alert**, and then select **Next**.
7. On the **Which performance counters would you like to monitor?** page, select **Add**.
8. In the **Available counters** list, expand **Processor**, select **% Processor Time**, select **Add**, and then select **OK**.
9. On the **Which performance counters would you like to monitor?** page, in the **Alert when** list, select **Above**.
10. In the **Limit** box, enter **10**, and then select **Next**.
11. On the **Create the data collector set?** page, select **Finish**.
12. In the navigation pane, expand the **User Defined** node, and then select **SEA-ADM1 Alert**.
13. In the results pane, right-click or access the context menu for **DataCollector01**, and then select **Properties**.
14. In the **DataCollector01 Properties** dialog box, enter **1** in the **Sample interval** box, and then select the **Alert Action** tab.
15. Select the **Log an entry in the application event log** check box, and then select **OK**.
16. In the navigation pane, right-click or access the context menu for **SEA-ADM1 Alert**, and then select **Start**.

25.0.5.4 Task 4: Introduce additional workload on the server

1. On **SEA-ADM1**, open File Explorer.
2. Browse to **C:\Labfiles\Mod11**.
3. Double-click or select **CPUSTRES64.EXE**, and then select Enter.
4. In the **CPU Stress - Sysinternals:www.sysinternals.com** dialog box, right-click or access the context menu for the highlighted thread at the top of the list of running threads, select **Activity Level**, and then select **Busy (75%)**.
5. After a minute, close CPUSTRES64 and File Explorer.

25.0.5.5 Task 5: Verify the results

1. Switch to **SEA-CL1**.
2. In **Event Viewer**, expand **Windows Logs** in the navigation pane.
3. Select **Forwarded Events**.

Question: Are there any performance-related alerts?

25.1 Answer: Answers might vary, but there should be some events that relate to the workload imposed on SEA-ADM1. Events will have an ID of 2031.

25.2 lab: title: 'Lab: Migrating server workloads' type: 'Answer Key' module: 'Module 12: Upgrade and migration in Windows Server'

26 Lab answer key: Migrating server workloads

26.1 Exercise 1: Selecting a process to migrate server workloads

26.1.1 Task 1: Study the scenario

1. Study the lab scenario.
2. Study the exercise scenario.

26.1.2 Task 2: Plan how to update domain controllers to Windows Server 2019

Answer the following questions based on the scenario:

1. To implement domain controllers running Windows Server 2019, should you upgrade the existing Active Directory Domain Services (AD DS) forest or migrate to a new AD DS forest?

   Answer: It's rare to migrate to a new AD DS forest. If your main goal is to update domain controllers to a new version of Windows Server, you should update AD DS in the existing by adding domain controllers running Windows Server 2019. You should only consider migrated to a new AD DS forest when restructuring of domains or forests is required. For example, when two companies merge, the AD DS forest of one company might be migrated into the other.

2. What are the highest domain and forest functional levels that you can implement?

   Answer: The highest domain and forest functional levels that you can implement are Windows Server 2016. There is no Windows Server 2019 functional level.

3. Which domain controller operating systems can you use to implement the highest possible domain and forest functional levels?

   Answer: You can use domain controllers running Windows Server 2016 and Windows Server 2019 in a domain or forest at the Windows Server 2016 functional level.

4. What steps do you need to take before adding domain controllers running Windows Server 2019 to an existing AD DS forest?

   Answer: If you have the correct permissions, you don't need to perform any steps before you install the first domain controller running Windows Server 2019. The domain controller promotion process automatically prepares the forest and domain. However, you do have the option to prepare the domain and forest manually. To prepare the AD DS forest you run Adprep /forestprep. Then you can prepare the domain by running Adprep /domainprep. In a multidomain environment, you need to prepare each domain.

5. What do you need to consider when removing domain controllers running previous Windows Server versions?

   Answer: For normal domain authentication, domain controllers are located by using DNS records. Those DNS records automatically update when domain controllers are added or removed. So, basic authentication doesn't require any special steps when removing a domain controller. However, because domain controllers are often used for DNS you need to ensure that clients and servers are updated to use the IP addresses of the new domain controllers. Additionally, some apps are configured to use specific domain controllers as Lightweight Directory Access Protocol (LDAP) servers for authentication. Those apps also need to be reconfigured with the IP address or name of new domain controllers.

26.1.3 Task 3: Plan how to migrate other server workloads

Answer the following questions based on the scenario:

1. What steps do you need to perform before running the Windows PowerShell cmdlets in the Windows Server Migration Tools on Windows Server 2019.

Answer: To use the Windows Server Migration Tools on Windows Server 2019 you need to install the Windows Server Migration Tools feature. Then before you can use the cmdlets, you need to load the Windows PowerShell snap-in containing the cmdlets by running Add-PSSnapin Microsoft. Windows.Windows.ServerManager.Migration at a Windows PowerShell prompt.

2. What steps do you need to perform on a source server running Windows Server 2012 R2 before you can use the Windows PowerShell cmdlets in the Windows Server Migration Tools?

   Answer: To install the Windows Server Migration Tools on a down-level server, you need to run SmigDeploy.exe to create a deployment folder for that specific operating system. The deployment folder copies to the source server and installs by running SmigDeploy.exe from the deployment folder. Then you can load the snap-in for the Windows Server Migration Tools at a Windows PowerShell prompt on the source server.

3. Which cmdlet can you use to verify which features can be migrated from a source server?

   Answer: The Get-SmigServerFeature cmdlet lists the Windows features that can be migrated from either a local computer or a migration stored.

4. List the high-level steps for using the Windows Server Migration Tools to migrate settings from a source server to a destination server.

   Answer: To migrate feature configuration from a source server to a destination server, you begin by installing the feature on the target server. Then you run Export-SmigServerSetting on the source server and Import-SmigServerSetting on the destination server.

26.2 Exercise 2: Planning how to migrate files by using Storage Migration Service

26.2.1 Task 1: Study the scenario

1. Study the lab scenario.
2. Study the exercise scenario.

26.2.2 Task 2: Plan the migration of file servers

Answer the following questions based on the scenario:

1. Can you use Storage Migration Service to migrate files shares from Windows Server 2003 to Windows Server 2019?

   Answer: Yes, Storage Migration Service supports migrating file shares from Windows Server 2003 or newer versions of Windows Server.

2. Can you use Storage Migration Service to migrate files on Linux servers?

   Answer: Yes, if the source Linux servers are providing file shares accessible to Windows clients by using Samba. Storage Migration Service can't migrate files on Linux servers using only NFS.

3. Can you use Storage Migration Service to combine multiple file servers to a single new server?

   Answer: No. Storage Migration Service doesn't have the ability to merge the identities of multiple servers onto a single server.

4. Can you use Storage Migration Service to migrate file shares to a virtual machine in Azure?

   Answer: Yes. Storage Migration Service can migrate file shares to a virtual machine in Azure. If Azure is properly configured, Storage Migration Service can create the virtual machine automatically based on specifications that you provide.

26.2.3 Task 3: Plan how to use Storage Migration Service

Answer the following questions based on the scenario:

1. What software do you need to install to use Storage Migration Service?

   Answer: To use Storage Migration Service, you need to install the Storage Migration Service feature on the orchestrator server. On the destination server running Windows Server 2019, you should also install the Storage Migration Service Proxy feature. No software needs to install on the source server.

2. What firewall configuration do you need to implement to use Storage Migration Service?

   Answer: The Storage Migration Service needs to copy data and configure the source and destination servers. When you install the Storage Migration Service Proxy on a destination server, the firewall is configured automatically, but you should verify. On source and destination server, the following firewall rules must be enabled: File and Printer Sharing (SMB-In), Netlogon Service (NP-In), Windows Management Instrumentation (DCOM-In), Windows Management Instrumentation (WMI-In). On the orchestrator server, the File and Printer Sharing (SMB-In) rule needs to be enabled.

3. What accounts and permissions must be configured to use Storage Migration Service?

   Answer: To perform the migrations, you can use a single account that has administrator permissions on the source server, the orchestrator server, and the destination server. Alternatively, you can split the accounts into a source migration account and a destination migration account. A source migration account needs to have administrator permissions on the source server and the orchestrator server. A destination migration account needs to have administrator permissions in the destination server and the orchestrator server.

4. Which tool do you use to create and manage jobs?

   Answer: Storage Migration Service jobs are created and managed from Windows Admin Center in the Storage Migration Service node.

5. What is the relationship between volumes in the source server and the destination server?

   Answer: A volume on the source server maps to a volume on the target server. If there are three source volumes, there must be three destination volumes. There is no logic for renaming folders with conflicting names.

6. After cutover, which identity information moves from the source server to the destination server?

   Answer: The name and IP addresses of the source server are moved to the destination server. The source server is renamed and give a new IP address.

7. Which data won't be migrated from the source server to the destination server?

   Answer: Storage Migration Service can't copy locked files. So, if users have a file open during a copy attempt, the file won't be migrated. Previous versions of files also aren't migrated.