Contents

1 WS-012T00: Windows Server 2019 Hybrid and Azure IaaS

- **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, we will need to make frequent updates to the course content to keep it current with the Azure services used in the course. We are publishing the lab instructions and lab files on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the Azure platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Azure changes and you find it first during a live delivery, go ahead and make an enhancement right in the lab source. Help your fellow MCTs.

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.
- It will be recommended that for every delivery, trainers check GitHub for any changes that may have been made to support the latest Azure services, and get the latest files for their delivery.

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 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repro, Microsoft and the course author will triage and include content and lab code changes as needed.
- You can submit bugs, changes, improvement and ideas. Find a new Azure feature before we have? Submit a new demo!

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. An explanation to the student regarding why they are receiving separate Lab instructions can highlight the nature of an always-changing cloud-based interface and platform. 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 | sort:"name" | 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-012T00-Windows-Server-2019-Hybrid-and-Azure-IaaS/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 lab: title: 'Lab: Implementing integration between AD DS and Azure AD' module: 'Module 2: Implementing Identity in Hybrid Scenarios'

3 Lab: Implementing integration between AD DS and Azure AD

3.1 Scenario

To address concerns regarding management and monitoring overhead resulting from using Microsoft Azure Active Directory (Azure AD) to authenticate and authorize access to Azure resources, you decide to test integration between on-premises Active Directory Domain Services (AD DS) and Azure AD to verify that this will address business concerns about managing multiple user accounts by using a mix of on-premises and cloud resources.

Additionally, you want to make sure that your approach addresses the Information Security team's concerns and preserves existing controls applied to Active Directory users, such as sign-in hours and password policies. Finally, you want to identify Azure AD integration features that allow you to further enhance on-premises Active Directory security and minimize its management overhead, including Azure AD Password Protection for Windows Server Active Directory and Self-Service Password Reset (SSPR) with password writeback.

Your goal is to implement pass-through authentication between on-premises AD DS and Azure AD.

3.2 Objectives

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

- Prepare Azure AD for integration with on-premises AD DS, including adding and verifying a custom domain.
- Prepare on-premises AD DS for integration with Azure AD, including running IdFix DirSync Error Remediation Tool, and configuring user principal name (UPN) suffixes.
- Install and configure Azure AD Connect.
- Verify integration between AD DS and Azure AD by testing the synchronization process.
- Implementing Azure AD integration features in Active Directory, including Azure AD Password Protection for Windows Server Active Directory and SSPR with password writeback.

3.3 Estimated time: 60 minutes

3.4 Lab setup

Virtual machines: **SEA-DC1** and **SEA-SVR2** virtual machines (VMs) must be running. Other VMs can be running, but they aren't required for this lab.

You should sign in to **SEA-SVR2** as **Contoso\Administrator** by using the following credentials:

- Username: **CONTOSO\Administrator**
- Password: **Pa55w.rd**

For this lab, you'll use the available VM environment and an Azure subscription. Before you begin the lab, ensure that you have an Azure subscription and a user account with an Owner or Contributor role in your subscription.

3.5 Exercise 1: Preparing Azure AD for AD DS integration

3.5.1 Scenario

You need to ensure that your Azure AD environment is ready for integration with your on-premises AD DS. Therefore, you'll create and verify a custom Azure AD domain name and an account with the Global Administrator role.

The main tasks for this exercise are:

1. Create a custom domain name in Azure.
2. Create a user with the Global Administrator role.
3. Reset the password for the user with the Global Administrator role.

3.5.2 Task 1: Create a custom domain name in Azure

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Azure portal.
2. Use the credentials that you instructor provides to sign in to the Azure portal.
3. In the Azure portal, browse to **Azure Active Directory**.
4. On the **Azure Active Directory** page, select **Custom domain names**, and then add `contoso.com`.
5. Review the DNS record types that you would use to verify the domain, and then close the pane without verifying the domain name.

   Note: The domain name provided might not be a valid domain. While you would use DNS records to verify a domain, this lab doesn't require that verification step.

3.5.3 Task 2: Create a user with the Global Administrator role

1. On **SEA-SVR2**, on the **Azure Active Directory** page in the Azure portal, select **Users**.
2. On the **All Users** page, select **New User**.
3. On the **New User** page, for the **User name** and **Name** text boxes under **Identity**, enter **admin**.

   Note: Ensure the domain name drop-down menu for the **User name** lists the default domain name ending with `onmicrosoft.com`. Also, make note of the password as you'll use it later.

1. Under **Groups and roles**, next to **Roles**, select **User**.
2. In the **Directory roles** page, in the list of roles, select **Global administrator**, and then select **Select**.
3. On the **New user** page, select **Create**.

3.5.4 Task 3: Reset the password for the user with the Global Administrator role

1. On the **Azure portal** page, select your user account and then select **Sign out**.
2. On the **Pick an account** page, select **Use another account**.
3. On the **Sign in** page, enter the fully-qualified username of the user account you previously created, and then select **Next**.
4. For the current password, use the password that you wrote down in the previous step.
5. Enter **Pa55w.rdPa55w.rd** as the new password, and then select **Sign in**.

   Note: The Azure portal might not allow using a shorter password when updating.

3.6 Exercise 2: Preparing on-premises AD DS for Azure AD integration

3.6.1 Scenario

You need to ensure that your existing Active Directory environment is ready for Azure AD integration. Therefore, you'll run the IdFix tool, and then ensure that the UPNs of the Active Directory users match the Azure AD tenant's custom domain name.

The main tasks for this exercise are:

1. Install IdFix.
2. Run IdFix.

3.6.2 Task 1: Install IdFix

1. On **SEA-SVR2**, open Microsoft Edge, and then browse to **https://github.com/microsoft/idfix**.
2. On the **Github** page, under **ClickOnce Launch**, select **launch**.
3. In the **IdFix Privacy Statement** dialog box, review the disclaimer, and then select **OK**.

3.6.3 Task 2: Run IdFix

1. In the **IdFix** window, select **Query**.
2. Review the list of objects from the on-premises Active Directory, and observe the **ERROR** and **ATTRIBUTE** columns. In this scenario, the value of **displayName** for **ContosoAdmin** is blank, and the tool's recommended new value appears in the attribute column.
3. In the **IdFix** window, in the **ACTION** drop-down menu, select **Edit**, and then select **Apply** to automatically implement the recommended changes.
4. In the **Apply Pending** dialog box, select **Yes**, and then close the IdFix tool.

3.7 Exercise 3: Downloading, installing, and configuring Azure AD Connect

3.7.1 Scenario

Exercise scenario: You're now ready to implement the integration by downloading Azure AD Connect, installing it on **SEA-SVR2**, and configuring its settings to match the integration objective.

The main task for this exercise is:

- Install and configure Azure AD Connect.

3.7.2 Task 1: Install and configure Azure AD Connect

1. On **SEA-SVR2**, open Microsoft Edge, browse to the Microsoft website, and search for "Install Azure AD Connect" to find the **Microsoft Azure Active Directory Connect** page.
2. On the **Microsoft Azure Active Directory Connect** page, select **Download**.
3. On the **Microsoft Azure Active Directory Connect** page, select the **I agree to the license terms and privacy notice** check box, and then select **Continue**.
4. On the **Express Settings** page, select **Use express settings**.
5. On the **Connect to Azure AD** page, enter the username and password of the Global Administrator account you created in exercise 1, and then select **Next**.
6. On the **Connect to AD DS** page, enter the following credentials, and then select **Next**:

- Username: **CONTOSO\Administrator**
- Password: **Pa55w.rd**

1. On the **Azure AD sign-in configuration** page, verify that the new domain you added is in the list of Active Directory UPN Suffixes.

   Note: The domain name provided might not be a verified domain. While you typically must verify a domain prior to installing Azure AD Connect, this lab doesn't require that verification step.

1. Select the **Continue without matching all UPN suffixes to verified domains** check box, and then select **Next**.
2. On the **Ready to configure** page, review the list of actions, and then select **Install**.

3.8 Exercise 4: Verifying integration between AD DS and Azure AD

3.8.1 Scenario

Now you have have installed and configured Azure AD Connect, you must verify its synchronization mechanism. You plan to make changes to an on-premises user account, which will trigger synchronization, and then you'll verify that the change replicated to the corresponding Azure AD user object.

The main tasks for this exercise are:

1. Verify synchronization in the Azure portal.
2. Verify synchronization in the Synchronization Service Manager.
3. Update a user account in Active Directory.
4. Create a user account in Active Directory.
5. Sync changes to Azure AD.
6. Verify changes in Azure AD.

3.8.2 Task 1: Verify synchronization in the Azure portal

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Azure portal.
2. Sign in to the portal by using the credentials for the account you created in exercise 1.
3. In the Azure portal, open **Azure Active Directory**.
4. On the **Azure Active Directory** page, select **Azure AD Connect**.
5. On the **Azure AD Connect** page, review the information under **Provision from Active Directory**.
6. On the **Azure Active Directory** page, select **Users**.
7. Observe the list of users that synced from on-premises Active Directory.

Note: When you begin directory synchronization, it can take 15 minutes for Active Directory objects to appear in the Azure AD portal.

1. In Microsoft Edge, select the **Back** button.
2. On the **Azure Active Directory** page, select **Groups**.
3. Observe the list of groups that synced from on-premises Active Directory.

3.8.3 Task 2: Verify synchronization in the Synchronization Service Manager

1. On **SEA-SVR2**, on the **Start** menu, expand **Azure AD Connect**, and then select **Synchronization Service**.
2. In the **Synchronization Service Manager** window, under the **Operations** tab, observe the tasks that were performed to sync the Active Directory objects.
3. Select the **Connectors** tab, and then observe the two connectors.

   Note: One of the connectors is for the on-premises Active Directory and the other is for the Azure domain.

1. Close the **Synchronization Service Manager** window.

3.8.4 Task 3: Update a user account in Active Directory

1. On **SEA-SVR2**, in **Server Manager**, open **Active Directory Users and Computers**.
2. In **Active Directory Users and Computers**, expand the **Sales** organizational unit (OU), and then open the properties for **Ben Miller**.
3. In the properties of the user, select the **Organization** tab.
4. In the **Job Title** text box, enter **Manager**, and then select **OK**.

3.8.5 Task 4: Create a user account in Active Directory

- Create the following user in the **Sales** OU:
  - First name: **Jordan**
  - Last name: **Mitchell**
  - User logon name: **Jordan**
  - Password: **Pa55w.rd**

3.8.6 Task 5: Sync changes to Azure AD

1. On **SEA-SVR2**, on the **Start** menu, select **Windows PowerShell**.
2. In the **Windows PowerShell** window, enter the following command, and then select Enter:

   ```
   Start-ADSyncSyncCycle
   ```

   Note: When you begin directory synchronization, it can take 15 minutes for Active Directory objects to appear in the Azure AD portal.

3.8.7 Task 6: Verify changes in Azure AD

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Azure portal.
2. On the **Azure Active Directory** page, select **Users**.
3. On the **All Users** page, search for the user **Ben**.
4. Open the properties page of the user **Ben Miller**, and then verify the updated attribute that synced from Active Directory.
5. In Microsoft Edge, select the **Back** button.
6. On the **All Users** page, search for the user **Jordan**.
7. Open the properties page of the user **Jordan Mitchell**, and then verify the attributes that synced from Active Directory.

3.9 Exercise 5: Implementing Azure AD integration features in AD DS

3.9.1 Scenario

You want to identify Azure AD integration features that will allow you to further enhance your on-premises Active Directory security and minimize its management overhead. You also want to implement Azure AD Password Protection for Windows Server Active Directory and self-service password reset with password writeback.

The main tasks for this exercise are:

1. Enable self-service password reset in Azure.
2. Enable password writeback in Azure AD Connect.
3. Enable pass-through authentication in Azure AD Connect.
4. Verify pass-through authentication in Azure.
5. Install and register the Azure AD Password Protection proxy service and DC agent.
6. Enable password protection in Azure.

3.9.2 Task 1: Enable self-service password reset in Azure

1. On **SEA-SVR2**, in the Azure portal, on the **Azure Active Directory** page, select **Password reset**.
2. On the **Password reset** page, select **Get a free Premium trial to use this feature**.
3. On the **Activate** page, under **AZURE AD PREMIUM P2**, select **Free trial**, and then select **Activate**.
4. Sign out, and then sign in to **SEA-SVR2** by using the following credentials:
   - Username: **CONTOSO\Administrator**
   - Password: **Pa55w.rd**
5. Start Microsoft Edge, and then navigate to the Azure portal.
6. Sign in to the portal by using the credentials for the account you created in exercise 1.
7. In the Azure portal, in the **Search resources, services, and docs** text box, enter **Azure Active Directory**, and then in the drop-down menu, select **Azure Active Directory**.
8. On the **Azure Active Directory** page, select **Password reset**.
9. On the **Password reset** page, observe how you can select the scope of users to which to apply the configuration.

   Note: Don't enable the password reset feature because it will break the configuration steps that are required later in this lab.

3.9.3 Task 2: Enable password writeback in Azure AD Connect

1. On **SEA-SVR2**, open **Azure AD Connect**.
2. In the **Microsoft Azure Active Directory Connect** window, select **Configure**.
3. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter the username and password of the user account you created in exercise 1, and then select **Next**.
5. On the **Connect your directories** page, select **Next**.
6. On the **Domain and OU filtering** page, select **Next**.
7. On the **Optional features** page, select **Password writeback**, and then select **Next**.

   Note: Password writeback is required for self-service password reset. This allows passwords changed by users in Azure AD to sync to the on-premises Active Directory.

1. On the **Ready to configure** page, review the list of actions to be performed, and then select **Configure**.
2. On the **Configuration complete** page, select **Exit**.

3.9.4 Task 3: Enable pass-through authentication in Azure AD Connect

1. On **SEA-SVR2**, on the **Start** menu, expand **Azure AD Connect**, and then select **Azure AD Connect**.
2. In the **Microsoft Azure Active Directory Connect** window, select **Configure**.
3. On the **Additional tasks** page, select **Change user sign-in**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter the username and password of the user account you created in exercise 1, and then select **Next**.
5. On the **User sign-in** page, select **Pass-through authentication**.
6. Verify that the **Enable single sign-on** check box is selected, and then select **Next**.
7. On the **Enable single sign-on** page, select **Enter credentials**.
8. In the **Forest credentials** dialog box, enter the following credentials, and then select **OK**:
   - Username: **Administrator**
   - Password: **Pa55w.rd**
9. On the **Enable single sign-on** page, verify that there's a green check mark next to **Enter credentials**, and then select **Next**.
10. On the **Ready to configure** page, review the list of actions to be performed, and then select **Configure**.
11. On the **Configuration complete** page, select **Exit**.

3.9.5 Task 4: Verify pass-through authentication in Azure

1. On **SEA-SVR2**, on the **Azure Active Directory** page in the Azure portal, select **Azure AD Connect**.
2. On the **Azure AD Connect** page, review the information under **User Sign-In**.
3. Under **User Sign-In**, select **Seamless single sign-on**.
4. On the **Seamless single sign-on** page, review the on-premises domain name.
5. In Microsoft Edge, select the **Back** button to return to the previous page.
6. In the Azure portal, on the **Azure Active Directory** page, select **Azure AD Connect**.
7. On the **Azure AD Connect** page, under **User Sign-In**, select **Pass-through authentication**.
8. On the **Pass-through authentication** page, review the list of servers under **Authentication Agent**.

   Note: To install the Azure AD Authentication Agent on multiple servers in your environment, open the **Azure AD Connect** page from the server, and then choose the **Download** option to install it on other servers.

3.9.6 Task 5: Install and register the Azure AD Password Protection proxy service and DC agent

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Microsoft website, and search for "Azure AD Password Protection for Windows Server Active Directory" to find the **Azure AD Password Protection for Windows Server Active Directory** page.
2. On the **Azure AD Password Protection for Windows Server Active Directory** page, download the **AzureADPasswordProtectionProxySetup.exe** and the **AzureADPasswordProtectionDCAgentSetup.msi** files to the server.

   Note: We recommend installing the proxy service on a server that isn't a domain controller.
3. Open the **AzureADPasswordProtectionProxySetup.exe** file to install the proxy service.
4. In the **Azure AD Password Protection Proxy Bundle Setup** window, select the **I agree to the license terms and conditions** check box, and then select **Install**.
5. In the **Installation Successfully Completed** window, select **Close**.
6. To install the DC agent, open the **AzureADPasswordProtectionDCAgentSetup.msi** file.

7. In the **Azure AD Password Protection DC Agent Setup** window, select the **I agree to the license terms and conditions** check box, and then select **Install**.
8. In the **Completed the Azure AD Password Protection DC Agent Setup Wizard** window, select **Finish**.
9. In the **Azure AD Password Protection DC Agent Setup** window, select **No**.
10. On the **Start** menu, select **Windows PowerShell**.
11. In Windows PowerShell, enter the following command, and then select Enter:

    ```
    Get-Service AzureADPasswordProtectionProxy | fl
    ```

12. Verify that the status is **Running**.
13. To register the proxy service with Azure AD, enter the following command, and then select Enter:

    ```
    Register-AzureADPasswordProtectionProxy -AccountUpn <NewUser>
    ```

    Note: Replace <NewUser> with the fully-qualified user principal name of the account you created in exercise 1.
14. In the authentication window, enter the credentials for the account, and then select **Sign in**.
15. To register the proxy service with on-premises Active Directory, in Windows PowerShell, enter the following command, and then select Enter:

    ```
    Register-AzureADPasswordProtectionForest -AccountUpn <NewUser>
    ```

    Note: Replace <NewUser> with the fully-qualified user principal name of the account you created in exercise 1.

3.9.7 Task 6: Enable password protection in Azure

1. On **SEA-SVR2**, in the Azure portal, on the **Azure Active Directory** page, select **Security**.
2. On the **Security** page, select **Authentication methods**.
3. On the **Authentication methods** page, select **Password protection**.
4. On the **Password protection** page, change the slider for **Enforce custom list** to **Yes**.
5. In the **Custom banned password list** text box, enter the following words (one per line):
   - Contoso
   - London

   Note: The list of banned passwords should be words that are relevant to your organization.
6. Confirm the slider for **Enable password protection on Windows Server Active Directory** is set to **Yes**.
7. Confirm the slider for **Mode** is set to **Audit**, and then select **Save**.

3.10 Exercise 6: Cleaning up

3.10.1 Scenario

You want to disable synchronization from the on-premises Active Directory to Azure. This will involve removing Azure AD Connect and disabling synchronization with Azure.

The main tasks for this exercise are:

1. Uninstall Azure AD Connect.
2. Disable directory synchronization in Azure.

3.10.2 Task 1: Uninstall Azure AD Connect

1. On **SEA-SVR2**, on the **Start** menu, select **Control Panel**.
2. In the **Control Panel** window, under **Programs**, select **Uninstall a program**.

3. In the **Uninstall or change a program** window, select **Microsoft Azure AD Connect**, and then select **Uninstall**.
4. In the **Programs and features** dialog box, select **Yes**.
5. In the **Uninstall Azure AD Connect** window, select **Remove**.
6. After the uninstall completes, in the **Uninstall Azure AD Connect** window, select **Exit**.
7.

3.10.3 Task 2: Disable directory synchronization in Azure

8. On **SEA-SVR2**, on the **Start** menu, select **Windows PowerShell**.
9. To install the Microsoft Online module for Azure AD, in Windows PowerShell, enter the following command, and then select Enter:

   ```
   Install-Module -Name MSOnline
   ```

10. When prompted to install the NuGet provider, enter **Y**, and then select Enter.
11. When prompted to install the modules from an untrusted repository, enter **Y**, and then select Enter.
12. In Windows PowerShell, enter the following to provide the credentials to Azure, and then select Enter:

    ```
    $msolcred=Get-Credential
    ```

13. In the **Windows PowerShell credential request** dialog box, enter the credentials of the user account you created in exercise 1, and then select **OK**.
14. In Windows PowerShell, enter the following to connect to Azure, and then select Enter:

    ```
    Connect-MsolService -Credential $msolcred
    ```

15. In Windows PowerShell, enter the following to disable directory synchronization in Azure, and then select Enter:

    ```
    Set-MsolDirSyncEnabled -EnableDirSync $false
    ```

16. When prompted to confirm, enter **Y**, and then select Enter.

3.11 lab: title: 'Lab: Using Windows Admin Center in hybrid scenarios' module: 'Module 3: Facilitating hybrid management and operational monitoring in hybrid scenarios'

4 Lab: Using Windows Admin Center in hybrid scenarios

4.1 Scenario

To address concerns regarding consistent operational and management model, regardless of the location of managed systems, you'll test the capabilities of Windows Admin Center in the hybrid environment containing different versions of Windows Server operating system running on-premises and in Azure VMs.

Your goal is to verify that Windows Admin Center can be used in a consistent manner regardless of the location of managed systems.

4.2 Objectives

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

- Test hybrid connectivity by using Azure Network Adapter.
- Deploy Windows Admin Center gateway in Azure.
- Verify functionality of Windows Admin Center gateway in Azure.

4.3 Estimated time: 90 minutes

4.4 Lab setup

Lab virtual machines: **SEA-CL1**, **SEA-DC1**, and **SEA-SVR2**

User name: **CONTOSO\Administrator** Password: **Pa55w.rd1234**

For this lab, you'll use SEA-CL1, SEA-DC1, and SEA-SVR2 lab virtual machines and an Azure subscription. Before you begin the lab, complete the following steps:

1. Ensure that you have an Azure subscription and a user account with the Owner or Contributor role in that subscription.
2. Start SEA-CL1, SEA-DC1 and SEA-SVR2.

4.5 Exercise 1: Provisioning Azure VMs running Windows Server 2019

4.5.1 Scenario

You need to verify that you can establish hybrid connectivity between an on-premises server and an Azure virtual network. To start, you'll provision Azure VMs running Windows Server 2019 by using an ARM template.

The main tasks for this exercise are as follows:

1. Create an Azure resource group by using an Azure Resource Manager template.
2. Create an Azure VM by using an Azure Resource Manager template.

4.5.2 Task 1: Create an Azure resource group by using an Azure Resource Manager template

1. On SEA-CL1, start Microsoft Edge, navigate to the Azure portal, and sign in by using credentials of a user account with the Owner role in the subscription you'll be using in this lab.
2. In the Azure portal, open a PowerShell session in the **Cloud Shell** blade.
3. Upload the file **M03-lab-sub_template.json** , which can be found at C:\Labfiles\Mod03 into the Cloud Shell home directory.
4. From the Cloud Shell blade, run the following to create a resource group that will contain resources you provision in this lab Replace the `<Azure region>` placeholder with *eastus*:

```
$location = '<Azure region>'
New-AzSubscriptionDeployment `
  -Location $location `
  -Name ws2019-m031subDeployment `
  -TemplateFile $HOME/M03-lab-sub_template.json `
  -rgLocation $location `
  -rgName 'ws2019-m031-rg'
```

> **Note**: This lab has been tested and verified using East US, so you should use that region. In general, to identify Azure regions where you can provision Azure VMs, refer to Find Azure credit offers in your region.

4.5.3 Task 2: Create an Azure VM by using an Azure Resource Manager template

1. From the Cloud Shell blade, upload an Azure Resource Manager template **M03-lab-rg_template.json** and a parameter file **M03-lab-rg_template.parameters.json**.
2. From the Cloud Shell blade, run the following to deploy a Azure VM running Windows Server 2019 that you'll be using in this lab:

```
New-AzResourceGroupDeployment `
  -Name ws2019-m031rgDeployment `
  -ResourceGroupName 'ws2019-m031-rg' `
  -TemplateFile $HOME/M03-lab-rg_template.json `
  -TemplateParameterFile $HOME/M03-lab-rg_template.parameters.json
```

> **Note**: Wait for the deployment to complete before you proceed to the next exercise. The deployment should take less than 5 minutes.

3. Review the ws2019-m03-vnet subnets. If there is no gateway subnet, then create a Gateway subnet using 10.3.3.224/27.

4.6 Exercise 2: Implementing hybrid connectivity by using the Azure Network Adapter

4.6.1 Scenario

You need to verify that you can establish hybrid connectivity between an on-premises server and the Azure VM you provisioned in the previous exercise. You'll use for this purpose the Azure Network Adapter feature of Windows Admin Center.

The main tasks for this exercise are as follows:

1. Register Windows Admin Center with Azure.
2. Create an Azure Network Adapter.

4.6.2 Task 1: Register Windows Admin Center with Azure

1. On SEA-CL1, start Microsoft Edge and connect to Windows Admin Center running on SEA-SVR2.
2. From the Windows Admin Center page, attempt to add an Azure Network Adapter.
3. When prompted, register Windows Admin Center to the Azure subscription you used in the previous exercise.

4.6.3 Task 2: Create an Azure Network Adapter

1. On SEA-CL1, in the Microsoft Edge window displaying Windows Admin Center running on SEA-SVR2 attempt to create an Azure Network Adapter again.
2. Create an Azure Network Adapter with the following settings:

Table 1: Azure Network Adapter settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Location	eastus
Virtual network	ws2019-m03-vnet
Gateway subnet	10.3.3.224/27
Gateway SKU	VpnGw1
Client Address Space	192.168.0.0/24
Authentication Certificate	Auto-generated Self-signed root and client Certificate

3. On SEA-CL1, switch to the Microsoft Edge window displaying the Azure portal and verify that a new virtual network gateway with the name starting with **WAC-Created-vpngw-** is being provisioned.
4. On SEA-CL1, in the Microsoft Edge window displaying the Windows Admin Center running on SEA-SVR2, verify that you see a new network adapter named **WACVPN-26123** representing the Point-to-Site VPN connection with the IPv4 address of **192.168.0.1**.

   Note: The provisioning of the Azure virtual network gateway can take up to 45 minutes. Do not wait for the provisioning to complete but instead proceed to the next exercise.

4.7 Exercise 3: Deploying Windows Admin Center gateway in Azure

4.7.1 Scenario

You need to evaluate the ability to manage Azure VMs running Windows Server OS by using Windows Admin Center. To accomplish this, you'll first install a Windows Admin Center gateway in the Azure virtual network you implemented in the first exercise of this lab.

The main tasks for this exercise are as follows:

1. Install Windows Admin Center gateway in Azure.
2. Review results of the script provisioning.

4.7.2 Task 1: Install Windows Admin Center gateway in Azure

1. On SEA-CL1, switch to the browser window displaying the the Azure portal.
2. Back in the Azure portal, start a PowerShell session in the **Azure Cloud Shell** blade.
3. From the Cloud Shell blade, upload the file **Deploy-WACAzVM.ps1** into the Cloud Shell home directory.
4. From the Cloud Shell blade, run the following to enable the compatibility for the **AzureRm** PowerShell cmdlets that are used by the Windows Admin Center provisioning script:

   ```
   Enable-AzureRmAlias -Scope Process
   ```

5. From the Cloud Shell blade, run the following to set values of variables necessary to run the the Windows Admin Center provisioning script:

   ```
   $rgName = 'ws2019-m031-rg'
   $vnetName = 'ws2019-m03-vnet'
   $nsgName = 'ws2019-m03-web-nsg'
   $subnetName = 'subnet1'
   $location = 'eastus'
   $pipName = 'wac-public-ip'
   $size = 'Standard_D2s_v3'
   $image = 'Win2019Datacenter'
   ```

6. From the Cloud Shell blade, run the following to set the script parameters variable:

   ```
   $scriptParams = @{
     ResourceGroupName = $rgName
     Name = 'ws2019-wac-vm'
     VirtualNetworkName = $vnetName
     SubnetName = $subnetName
     GenerateSslCert = $true
     size = $size
     image = $image
   }
   ```

7. From the Cloud Shell blade, run the following commands to disable certificate verification for PowerShell remoting.

   ```
   install-module pswsman
   Disable-WSManCertVerification -All
   ```

8. From the Cloud Shell blade, run the following to launch the provisioning script:

   ```
   ./Deploy-WACAzVM.ps1 @scriptParams
   ```

9. When prompted to provide the name for the local Administrator account, enter **Student**
10. When prompted to provide the password for the local Administrator account, enter **Pa55w.rd1234**

    Note: Wait for the provisioning script to complete. This might take about 5 minutes.

11. Verify that the script completed successfully and note the final message providing the URL for the connection to the Windows Admin Center.

4.7.3 Task 2: Review results of the script provisioning

1. In the Azure portal, navigate to the blade of the **ws2019-m031-rg** resource group.
2. On the **ws2019-m031-rg** blade, on the **Overview** blade, review the list of resources, including the Azure VM **ws2019-wac-vm**.
3. On the **ws2019-wac-vm | Networking** blade, on the **Inbound port rules** tab, note entries representing the inbound port rule allowing connectivity on TCP port 5986 and the inbound rule allowing connectivity on TCP port 443.

4.8 Exercise 4: Verifying functionality of the Windows Admin Center gateway in Azure

4.8.1 Scenario

With all required components in place, you'll test the WAC functionality targeting the Azure VMs deployed into the Azure virtual network you provisioned in the first exercise of this lab.

The main tasks for this exercise are as follows:

1. Connect to the Windows Admin Center gateway running in Azure VM.
2. Enable PowerShell Remoting on an Azure VM.
3. Connect to an Azure VM by using the Windows Admin Center gateway running in Azure VM.

4.8.2 Task 1: Connect to the Windows Admin Center gateway running in Azure VM

1. On SEA-CL1, start Microsoft Edge and connect the Windows Admin Center gateway running in the Azure VM you identified in the previous exercise.
2. When prompted, authenticate by using the following credentials:

Table 2: Sign in credentials

Setting	Value
Username	Student
Password	Pa55w.rd1234

3. On the **All connections** blade of the Windows Admin Center page, select **ws2019-wac-vm** [**Gateway**].
4. When prompted, authenticate by using the following credentials:

Table 3: Sign in credentials

Setting	Value
Username	Student
Password	Pa55w.rd1234

5. Examine the **Overview** blade of the Windows Admin Center page.

4.8.3 Task 2: Enable PowerShell Remoting on an Azure VM

1. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, navigate to the blade of the **ws2019-m03-vm0** Azure VM.
2. On the **ws2019-m03-vm0** blade, use the **Run Command** feature to run the following command:

   ```
   winrm quickconfig -quiet
   ```

3. On the **ws2019-m03-vm0** blade, use the **Run Command** feature to run the following command:

   ```
   Set-NetFirewallRule -Name WINRM-HTTP-In-TCP-PUBLIC -RemoteAddress Any
   ```

4. On the **ws2019-m03-vm0** blade, use the **Run Command** feature to run the following command:

   ```
   Enable-PSRemoting -Force -SkipNetworkProfileCheck
   ```

4.8.4 Task 3: Connect to an Azure VM by using the Windows Admin Center gateway running in Azure VM

1. On SEA-CL1, in the Microsoft Edge window displaying the interface of the Windows Admin Center gateway running on the **ws2019-wac-vm** Azure VM, add a connection to the Azure VM **ws2019-m03-vm0** Azure VM by using its IP address.
2. When prompted, authenticate by using the following credentials:

Table 4: Sign in credentials

Setting	Value
Username	Student
Password	Pa55w.rd1234

3. Once successfully connected, examine the **Overview** blade of the Windows Admin Center page on the **ws2019-wac-vm** Azure VM

4.9 Exercise 5: Deprovisioning the Azure environment

4.9.1 Scenario

To minimize Azure-related charges, you'll deprovision the Azure resources provisioned throughout this lab.

The main tasks for this exercise are as follows:

1. Start a PowerShell session in Cloud Shell.
2. Identify all Azure resources provisioned in the lab.

4.9.2 Task 1: Start a PowerShell session in Cloud Shell

1. On SEA-CL1, switch to the Microsoft Edge window displaying the Azure portal.
2. From the Azure portal, open a PowerShell session in **Azure Cloud Shell** blade.

4.9.3 Task 2: Identify all Azure resources provisioned in the lab

1. From the Cloud Shell blade, run the following to list all resource groups created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-03-m03'
   ```

2. From the Cloud Shell blade, run the following to delete all resource groups you created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-03-m03' | Remove-AzResourceGroup -Force -AsJob
   ```

4.9.4 Results

After completing this lab, you have deployed and configured Azure VMs running Windows Server 2019 in the manner that satisfies the Contoso's manageability and security requirements.

4.9.5 Prepare for the next module

4.10 End the lab when you're finished in preparation for the next module.

4.11 lab: title: 'Lab: Using Azure Security Center in hybrid scenarios' module: 'Module 4: Implementing Security Solutions in Hybrid Scenarios'

5 Lab: Using Azure Security Center in hybrid scenarios

5.1 Scenario

To identify Microsoft Azure security-related integration features with which you can further enhance your on-premises security environment, you have decided to add servers in your proof-of-concept environment to Security Center.

Your goal is to onboard on-premises servers that are running Windows Server 2019 into Security Center and then verify the hybrid capabilities of Security Center.

5.2 Objectives

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

- Configure Security Center.
- Onboard on-premises Windows Server 2019 computers into Security Center.
- Verify the hybrid capabilities of Security Center.

5.3 Estimated time: 45 minutes

5.4 Lab setup

Lab virtual machines: **SEA-CL1**, **SEA-DC1**, **SEA-SVR1**, and **SEA-SVR2** Username: **Administrator** Password: **Pa55w.rd**

For this lab, you'll use the available virtual machine (VM) environment and an Azure subscription. Before you begin the lab, complete the following steps:

1. Ensure that you have an Azure subscription and a user account with the Owner or Contributor role in that subscription.
2. Start the VMs.

5.5 Exercise 1: Provisioning Azure VMs running Windows Server 2019

5.5.1 Scenario

You must test Security Center functionality in hybrid scenarios, including its benefits for Azure VMs that are running Windows Server 2019. To start, you'll provision Azure VMs that are running Windows Server 2019 by using an Azure Resource Manager template.

The main tasks for this exercise are:

1. Start Azure Cloud Shell.
2. Create an Azure VM by using Resource Manager templates.

5.5.2 Task 1: Start Azure Cloud Shell

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with password **Pa55w.rd**.
2. Open Microsoft Edge, and then browse to the Azure portal.
3. Sign in by using the credentials that you created for this course.
4. In the Azure portal, select **Cloud Shell**.
5. Select **PowerShell**.
6. When prompted, verify that your subscription is chosen, and then select **Create storage**.

5.5.3 Task 2: Create an Azure VM by using Resource Manager templates

Upload the Resource Manager templates

1. In Cloud Shell, select **Upload/Download files**, and then select **Upload**.
2. Browse to the Desktop folder and then the **Allfiles\Labfiles\Mod04** folder.
3. Select the **M04-lab-rg_template.json** file, and then select **Open**.
4. Repeat steps 1 through 3 for the following files:
   - **M04-lab-rg_template.parameters.json**
   - **M04-lab-sub_template.json**

Create a resource group

1. In Cloud Shell, enter the following command, replacing *<region>* with an Azure region that's close to you:

   ```
   New-AzSubscriptionDeployment -Location '<region>' -Name ws2019-m04deployment -TemplateFile ./M04-la
   ```

Create a Windows Server VM

1. In Cloud Shell, enter the following command:

   ```
   New-AzResourceGroupDeployment -Name windows-m04rgDeployment -ResourceGroupName m04-rg -TemplateFil
   ```

2. Close Cloud Shell.
3. Wait for deployment to complete.

   Note: You can close Cloud Shell before deployment is complete.

5.6 Exercise 2: Configuring Azure Security Center

5.6.1 Scenario

You'll make Security Center available and upgrade to the Standard pricing tier. You'll then review the features and capabilities that apply to Windows Server hybrid scenarios.

The main tasks for this exercise are:

1. Make Security Center available and upgrade to the Standard pricing tier.
2. Turn on automatic provisioning of the Log Analytics agent.
3. Review the features and capabilities that apply to hybrid scenarios.

5.6.2 Task 1: Make Security Center available and upgrade to the Standard pricing tier

1. Open Microsoft Edge, and then verify that you're signed in to the Azure portal.
2. In the search box, enter **Security Center**, and then select **Security Center** from the results.
3. On the **Security Center** menu, select **Getting started**.
4. On the **Upgrade** tab of the **Getting started** pane, for **Enable standard tier on 1 subscriptions**, select your subscription.
5. Select **Upgrade**.

   Note: Your subscription may already be upgraded for Security Center in which case there will not be an upgrade button and you may continue with Task 2.

6. Select **Continue without installing agents**.

5.6.3 Task 2: Turn on automatic provisioning of the Log Analytics agent

1. Browse back to Security Center.
2. In Security Center, select **Pricing & settings**, select your subscription, and then select **Auto Provisioning**.
3. In the **Log Analytics agent for Azure VMs** section, select **On** if it is not already enabled.
4. In the **Workspace configuration** section, verify that **ASC default workspace** is selected, and then select **Save** if it is not already enabled.
5. Refresh the page, and then browse back to the **Auto Provisioning** page.
6. Verify that **Log Analytics agent for Azure VMs** is **On** and the **Description** indicates that security related configurations and events will be collected. Select **Edit Configuration** and verify **All Events** is selected. If not, select it and save the setting.

   Note: It might take up to 30 minutes for the **Log Analytics** workspace to be created after selecting **Save** in step 4. You might need to refresh the page several times before the option to select **All Events** is available. Continue only after you're able to select **All events** and save the setting.

5.6.4 Task 3: Review the features and capabilities that apply to hybrid scenarios

1. In the **General** section of Security Center, select **Inventory**.
2. Review the **Recommendation** list.

   Note: that the **Failed Resources** box indicates the type of resource to which the recommendation applies and lists how many resources the recommendation applies to.

3. Under the **Resource Name** column select the **ws2019-m04-vm0** VM.
4. Note the details of the VM's security health.
5. Close the **ws2019-m04-vm0** pane.
6. In the **Coud Security** section, select **Regulatory compliance**.
7. Under **Azure Security Benchmark**, select **expand all compliance controls**, and then review the assessments.

5.7 Exercise 3: Onboarding on-premises Windows Server 2019 into Azure Security Center

5.7.1 Scenario

You'll onboard **SEA-SVR1** into Security Center to determine the Security Center features that you can use to enhance security for Windows Server 2019, which is running in your on-premises environment.

The main task for this exercise is:

- Download and install the Log Analytics agent.

5.7.2 Task 1: Download and install the Log Analytics agent

1. On **SEA-CL1**, switch to Microsoft Edge, and then verify that you're signed in to the Azure portal.
2. In the search box, enter **Log Analytics**, and then select **Log Analytics workspaces** from the results.
3. Select the listed Log Analytics workspace. There should only be one, and the name will start with "DefaultWorkspace".
4. Select **Agents management**.
5. Copy and save the **WORKSPACE ID** and the **PRIMARY KEY**.

   Note: You can save these values in Notepad or make a note of them.
6. Select the **Download Windows Agent (64 bit)** link.
7. In the download status bar, on the context menu for **MMASetup-AMD64.exe**, select **Show in folder**.
8. Copy the file to **c:\labfiles\mod04**. Create the folder if needed.
9. Select **Start**, and then open Windows PowerShell.
10. In PowerShell, browse to **c:\labfiles\Mod04**.
11. Enter the following command:

    ```
    .\MMASetup-amd64.exe /c /t:c:\labfiles\mod04
    ```
12. Open a new tab in Microsoft Edge, open **Windows Admin Center**, and then sign in as **Administrator** with password **Pa55w.rd**.
13. Select **Add**.
14. Under **Windows Server**, select **Add**.
15. Under **Server name**, enter `sea-svr1.contoso.com`, and then select **Add**.
16. In **Windows Admin Center**, select **SEA-SVR1**, and then sign in as **Contoso\Administrator** with password **Pa55w.rd**.
17. Select **SEA-SVR1**, select **PowerShell**, and then enter password **Pa55w.rd**.
18. Enter the following commands:

    ```
    mkdir c:\labfiles\mod04
    copy \\SEA-CL1\c$\labfiles\mod04\*.* c:\labfiles\mod04\
    ```
19. Browse to **c:\labfiles\mod04**.
20. Enter the following command:

    ```
    .\setup.exe /qn NOAPM=1 ADD_OPINSIGHTS_WORKSPACE=1 OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIG
    ```

    where *<workspaceID>* is the WORKSPACE ID that you copied earlier and *<primarykey>* is the PRIMARY KEY that you copied earlier.
21. Wait for the installation to complete.

5.8 Exercise 4: Verifying the hybrid capabilities of Azure Security Center

5.8.1 Scenario

With a mix of on-premises Azure VMs and servers that are running Windows Server 2019, you want to validate the Security Center capabilities that are available in both cases. You'll simulate a cyberattack on both resources and be vigilant for alerts in Security Center.

The main tasks for this exercise are:

1. Validate the Security Center capabilities for Azure VMs.
2. Validate the Security Center capabilities for on-premises servers.

5.8.2 Task 1: Validate the Security Center capabilities for Azure VMs

1. Open Microsoft Edge, and then browse to the Azure portal.
2. Sign in by using the credentials that you created for this course.
3. In the search box, enter **Virtual Machines**, and then select **Virtual Machines** from the results.
4. Select the **ws2019-m04-vm0** VM, select **Connect**, select **RDP**, and then select **Download RDP File**.
5. In the download status bar, on the context menu for the **ws2019-mo4-vm0.rdp** file, select **Open**.
6. If prompted, select **Connect**.
7. Enter the username **Student** with password **Pa55w.rd1234**.
8. In the VM's Remote Desktop session, select **Start**, and then select **Windows PowerShell**.
9. Enter the following commands:

```
mkdir c:\temp
powershell -nop -exec bypass -EncodedCommand "cABvAHcAZQByAHMAaABlAGwAbAAgACOAYwBvAGOAbQBhAG4AZAAg
```

10. In Microsoft Edge, switch to the Azure portal tab.
11. In the search box, enter **Security Center**, and then select **Security Center** from the results.
12. On the **Overview** page, review the **Threat protection** section. You should have one new alert. If not, wait a few minutes.
13. In the **General** section of the **Security Center** menu, select **Security alerts**. There should be one alert.
14. In the **General** section of the **Security Center** menu, select **Inventory**.
15. Select the **ws2019-mo4-vm0** VM.
16. Review the recommendations.

5.8.3 Task 2: Validate the Security Center capabilities for on-premises servers

1. In Microsoft Edge, switch to the **Windows Admin Center** tab.
2. Verify that you're signed in to **SEA-SVR1** as **Contoso\Administrator**, and then select **PowerShell**.
3. Enter the following commands:

```
mkdir c:\temp
powershell -nop -exec bypass -EncodedCommand "cABvAHcAZQByAHMAaABlAGwAbAAgACOAYwBvAGOAbQBhAG4AZAAg
```

4. Open Microsoft Edge, and then browse to the Azure portal.
5. Sign in by using the credentials that you created for this course.
6. In the search box, enter **Security Center**, and then select **Security Center** from the results.
7. On the **Overview** page, review the **Azure defender** section. You should have one new alert for **SEA-SVR1**. If not, wait a few minutes.
8. In the **General** section of the **Security Center** menu, select **Security alerts**. There should be a new alert for **SEA-SVR1**.
9. In the **General** section of the **Security Center**, select **Inventory** and then select **SEA-SVR1**.

10. Review the recommendations for **SEA-SVR1**.

    Note: You might need to wait several minutes for **SEA-SVR1** to be listed.

5.9 Exercise 5: Deprovisioning the Azure environment

5.9.1 Scenario

To minimize Azure-related charges, you'll deprovision the Azure resources that were provisioned throughout this lab.

The main tasks for this exercise are:

1. Start a PowerShell session in Cloud Shell.
2. Identify and remove all Azure resources that were provisioned in the lab.
3. Prepare for the next module.

5.9.2 Task 1: Start a PowerShell session in Cloud Shell

1. On **SEA-CL1**, in Microsoft Edge, switch to the Azure portal.
2. Select **Cloud Shell**.

5.9.3 Task 2: Identify and remove all Azure resources that were provisioned in the lab

- In Cloud Shell, enter the following command to find and remove all resource groups:

  ```
  Get-AzResourceGroup | Remove-AzResourceGroup -Force
  ```

5.9.4 Task 3: Prepare for the next module

- End the lab.

5.10 Results

After completing this lab, you have:

- Configured Security Center.
- Onboarded on-premises servers that are running Windows Server 2019 into Security Center.
- Verified the hybrid capabilities of Security Center.

5.11 lab: title: 'Lab: Implementing Azure File Sync' module: 'Module 5: Implementing File Services in Hybrid Scenarios'

6 Lab: Implementing Azure File Sync

6.1 Scenario

To address concerns regarding Distributed File System (DFS) Replication between Contoso's London headquarters and its Seattle–based branch office, you decide to test Azure File Sync as an alternative replication mechanism between two on-premises file shares.

6.2 Objectives

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

- Implement DFS Replication in your on-premises environment.
- Create and configure a sync group.
- Replace DFS Replication with Azure File Sync based replication.
- Verify replication and enable cloud tiering.
- Troubleshoot replication conflicts.

6.3 Estimated time: 45 minutes

6.4 Lab setup

Virtual machines: **LON-SVR1**, **SEA-CL1**, **SEA-DC1**, **SEA-SVR1**, and **SEA-SVR2**

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

6.5 Exercise 1: Implementing DFS Replication in your on-premises environment

6.5.1 Scenario

Exercise scenario: Before you start testing an on-premises DFS Replication migration, you first need to implement DFS Replication in your proof-of-concept environment on **LON-SVR1** and **SEA-SVR1**.

The main tasks for this exercise are:

1. Deploy DFS.
2. Test DFS deployment.

6.5.2 Task 1: Deploy DFS

1. Sign in to **SEA-CL1** as **Contoso\Administrator** and use **Pa55w.rd** as the password. If in the Lab Setup the **Allfiles** folder was copied to the **Desktop**, then open the **Allfiles** folder, and copy the **Labfiles** folder to **C:**. Then share the **Labfiles** folder to **Everyone** with **Read** access.
2. In File Explorer, browse to the **C:\Labfiles\Mod05** folder, and then run **M05-DeployDFS.ps1**.

6.5.3 Task 2: Test DFS deployment

1. On **SEA-CL1**, run **DFS Management**, and then add the `\\Contoso.com\Root\` namespace and the **Branch1** replication group to display.
2. Verify that the `\\Contoso.com\Root\Data` folder has targets on **LON-SVR1** and **SEA-SVR1**. Note which folders are configured as the targets.
3. Verify that the **Branch1** replication group has two members, **LON-SVR1** and **SEA-SVR1**. Note which folders are replicated on each server.
4. Open two instances of File Explorer. In the first **File Explorer** window, connect to **\\LON-SVR1\Data**, and then in the second **File Explorer** window, connect to **\\SEA-SVR1\Data**.

   Note: Wait until the files are replicated and both the File Explorer windows record the same content.

5. Create a new file with your name in **\\LON-SVR1\Data**, and then confirm that the file replicates to **\\SEA-SVR1\Data** after a few seconds. This confirms that DFS Replication is working.

6.5.4 Results

After completing this exercise, you have a working DFS infrastructure. This includes DFS Replication, which replicates content between **LON-SVR1** and **SEA-SVR1**.

6.6 Exercise 2: Creating and configuring a sync group

6.6.1 Scenario

To prepare for migrating the DFS Replication environment to File Sync, you must first create and configure a File Sync group.

The main tasks for this exercise are:

1. Create an Azure file share.
2. Use an Azure file share.
3. Deploy Storage Sync Service and a File Sync group.

6.6.2 Task 1: Create an Azure file share

1. On **SEA-CL1**, open the Azure portal, and then authenticate with your Azure credentials.
2. In the Azure portal, create an Azure storage account in a resource group named **RG1**. You can use the default settings, but make sure that the storage account has a unique name. For example, you can specify the storage account name in the following format:<*YourLowercaseInitials*>*DDMMYY*; for example, **df150620** if your name is Devon Torres and you're creating the storage account on June 15, 2020. If that name is already taken, add another character to the name until the name is available.

   Note: Use the same region for deploying all resources in this lab.
3. In the storage account, create a file share named **share1**.

6.6.3 Task 2: Use an Azure file share

1. On **SEA-CL1**, upload the **C:\Labfiles\Mod05\File1.txt** file to **share1**.
2. In the Azure portal, create a snapshot of **share1**.
3. On **SEA-CL1**, mount **share1** to drive **Z** by using the connection script that the Azure portal provides.
4. In File Explorer, on the mounted drive, open the file named **File1.txt**, enter your name, and then save the file.
5. Use **Previous Versions** in File Explorer to restore the previous version of **File1.txt**.
6. Open **File1.txt**, and then verify that it doesn't include your name.

6.6.4 Task 3: Deploy Storage Sync Service and a File Sync group

1. On **SEA-CL1**, use the Azure portal to create an Azure File Sync resource named **FileSync1**. Use the same region and Resource Group as you used when deploying the storage account.

   Note: Deploying File Sync creates a Storage Sync Service resource.
2. Create a sync group named **Sync1** in the **FileSync1** Storage Sync Service. Use the storage account that you created earlier and **share1** as the Azure file share when creating **Sync1**.
3. Verify that no server is currently registered with **FileSync1**.

6.6.5 Results

After completing this exercise, you have a File Sync group. You also have the cloud endpoint mapped on **SEA-CL1** so that you can inspect the Azure file share content.

6.7 Exercise 3: Replacing DFS Replication with File Sync–based replication

6.7.1 Scenario

Now that you have all the necessary components in place, it's time to replace DFS Replication with File Sync–based replication.

The main tasks for this exercise are:

1. Add **SEA-SVR1** as a server endpoint.
2. Register **LON-SVR1** with File Sync.
3. Remove DFS Replication and add **LON-SVR1** as a server endpoint.

6.7.2 Task 1: Add SEA-SVR1 as a server endpoint

1. On **SEA-CL1**, in the Azure portal, download the File Sync agent for Windows Server 2019 (**StorageSyncAgent_WS2019.msi**), and then save it to the **C:\Labfiles** folder.

   Note: If you downloaded the file to the default location, you need to copy the file to the **C:\Labfiles** folder.
2. Open the **C:\Labfiles\Mod05\Install-FileSyncServerCore.ps1** file, update the value of the *$RG_name* variable with the name of the resource group to which you deployed **FileSync1** (replace everything inside <>, including < and >, but leave the apostrophe at the beginning and at the end), and then save the file.
3. Run **C:\Labfiles\Mod05\Install-FileSyncServerCore.ps1**. This script installs the File Sync agent on the remote Windows Server.

4. Wait while the script is running—it takes some time. When you get the **WARNING** output, copy the nine-character code in the warning output to the Clipboard.
5. In a new Microsoft Edge tab, browse to **https://microsoft.com/devicelogin**.
6. In Microsoft Edge, paste the code in the **Enter code** dialog box, sign in with your Azure credentials, and then close the Microsoft Edge tab.
7. In the Azure portal, refresh the registered servers in the **FileSync1** Storage Sync Service, and then point out that `SEA-SVR1.Contoso.com` is now registered.
8. In File Explorer, open **\\SEA-SVR1\Data**, and then point out that the folder doesn't contain **File1.txt**.
9. Use the Azure portal to add **D:\Data** on `SEA-SVR1.Contoso.com` as a server endpoint to **Sync1**.
10. Use File Explorer to verify that **File1.txt** is available on **\\SEA-SVR1\Data**.

    Note: You uploaded **File1.txt** to the **File1.txtAzure** file share, from where it was synced to **SEA-SVR1** by File Sync.

6.7.3 Task 2: Register LON-SVR1 with File Sync

1. On **SEA-CL1**, in the **C:\Labfiles\Mod05\Install-FileSyncServerCore.ps1** file, for the **$Server** variable, replace **SEA-SVR1** with **LON-SVR1**, and then save the file.
2. Run **C:\Labfiles\Mod05\Install-FileSyncServerCore.ps1**.
3. Wait while the script is running—it takes some time. When you get the **WARNING** output, copy the nine-character code in the warning output to the Clipboard.
4. In a new Microsoft Edge tab, browse to **https://microsoft.com/devicelogin**.
5. In Microsoft Edge, paste the code in the **Enter code** dialog box, sign in with your Azure credentials, and then close the Microsoft Edge tab.
6. Use the Azure portal to verify that `SEA-SVR1.Contoso.com` and `LON-SVR1.Contoso.com` are registered with the **FileSync1** Storage Sync Service.

6.7.4 Task 3: Remove DFS Replication and add LON-SVR1 as a server endpoint

1. On **SEA-CL1**, use **DFS Management** to delete the **Branch1** replication group.
2. Use the Azure portal to add **D:\Data** on `LON-SVR1.Contoso.com` as a server endpoint to **Sync1**.

6.7.5 Results

After completing this exercise, you'll have replaced DFS Replication with File Sync.

6.8 Exercise 4: Verifying replication and enabling cloud tiering

6.8.1 Scenario

Exercise scenario: You now need to verify that you have successfully replaced DFS Replication with File Sync, and after confirming this, you need to enable cloud tiering.

The main tasks for this exercise are:

1. Verify File Sync.
2. Enable cloud tiering.

6.8.2 Task 1: Verify File Sync

1. On **SEA-CL1**, use two instances of File Explorer. In the first File Explorer instance, connect to **\\LON-SVR1\Data**, and in the second File Explorer instance, connect to **\\SEA-SVR1\Data**.
2. Create a file with your last name in the **\\LON-SVR1\Data** folder.
3. Verify that after some time, the file with your last name also appears in the **\\SEA-SVR1\Data** folder.

   Note You removed DFS Replication in the previous exercise. File Sync replicated the file with your name.

6.8.3 Task 2: Enable cloud tiering

1. On **SEA-CL1**, use the Azure portal to browse to the **Sync1** sync group in the **FileSync1** Storage Sync Service.
2. In the Azure portal, enable cloud tiering for the `LON-SVR1.Contoso.com` endpoint in **Sync1**. Set the **free disk space** policy to **80** percent and the **date policy** to cache files that were accessed in last **7** days.
3. In the File Explorer instance that's connected to the **\\LON-SVR1\Data** folder, in the **details** pane, add the **Attributes** column by right-clicking or accessing the context menu for the **Title** column; for example, on **Name**, select **More**, and then select **Attributes**.

   Note: After some time, the files on **LON-SVR1** would automatically tier. You can trigger tiering immediately by running on LON-Cl1:

```
Enter-PSSession -computername lon-svr1
Import-Module "C:\Program Files\Azure\StorageSyncAgent\StorageSync.Management.ServerCmdlets.dll"
Invoke-StorageSyncCloudTiering -Path D:\data
```

4. Verify the attributes of the files. Additionally, verify the size on the disk for the **Windows Server 2016 Hybrid Cloud.pdf** file by reviewing its properties.

6.8.4 Results

After completing this exercise, you'll have a working File Sync replication and a configured cloud tiering.

6.9 Exercise 5: Troubleshooting replication issues

6.9.1 Scenario

Exercise scenario: Contoso relies heavily on its DFS Replication implementation. You must ensure that any replication issues, including replication conflicts, can be quickly identified and resolved. To do so, you'll simulate the most common replication issues in your proof-of-concept environment and test their resolutions.

The main tasks for this exercise are:

1. Monitor File Sync replication.
2. Test replication conflict resolution.

6.9.2 Task 1: Monitor File Sync replication

1. On **SEA-CL1**, use File Explorer to copy the **C:\Windows\INF** folder to **\\LON-SVR1\Data**. The folder will sync to the cloud endpoint, causing sync traffic.
2. In the Azure portal, browse to the **Sync1** sync group in the **FileSync1** Storage Sync Service.
3. In the **Server endpoint** section, verify that the **Health** of both endpoints has green check marks.
4. Select the `LON-SVR1.Contoso.com` endpoint, in the **Server Endpoint Properties** pane, review **Sync Activity**, and then close the pane.
5. Select the **Files Synced** graph, and then explore how you can customize the graph by using a filter.
6. Verify if the **INF** folder is syncing to drive **Z**.
7. In the Azure portal, verify that the **INF** sync traffic is visible in the **Files Synced** and **Bytes Synced** graphs. The **INF** folder has more than 800 files, and its size is more than 40 megabytes (MB).

6.9.3 Task 2: Test replication conflict resolution

1. On **SEA-CL1**, in File Explorer, verify that **File1.txt** is available on **\\LON-SVR1\Data**. Remember that you uploaded **File1.txt** to the Azure file share, from where it was synced to **SEA-SVR1** by File Sync.
2. Create a file named **Sync.txt** on **\\LON-SVR1\Data**.
3. In File Explorer, verify that the **Sync.txt** file is also on drive **Z**. Remember that drive **Z** is the mounted Azure file share, where the file was synced from **LON-SVR1** by File Sync.
4. Create a file named **Demo.txt** on drive **Z**.
5. Create a file named **Demo.txt** on **\\LON-SVR1\Data**.

   Note: You're creating files with the same name to cause a sync conflict.

6. In File Explorer, review the content of drive **Z**. Verify that drive **Z**, which is the mounted Azure file share, consists of the **Demo.txt** and **Demo-LON-SVR1.txt** (or **Demo-Cloud.txt**) files. This is because File Sync detected sync conflict and added the endpoint name (**LON-SVR1**) to the file that caused the conflict.

   Note: You might need to wait up to a minute for the sync conflict to occur and for both files to appear on drive **Z**.

6.9.4 Results

After completing this exercise, you'll monitor File Sync replication and resolve replication conflicts.

6.10 Exercise 6: Cleaning up the Azure subscription

Exercise scenario: To minimize Azure-related charges, you will clean up the Azure subscription.

6.10.1 Task 1: Delete the Azure resources that were created in the lab

1. On **SEA-CL1**, use the Azure portal to browse to the **FileSync1** Storage Sync Service.
2. Remove `LON-SVR1.Contoso.com` and `SEA-SVR1.Contoso.com` as registered servers.
3. Delete the **share1** cloud endpoint in the **Sync1** sync group.
4. Delete the **Sync1** sync group.
5. Delete the **FileSync1** Storage Sync Service and the Azure storage account that you created in the lab (the storage account has a name in the *<YourLowercaseInitials>DDMMYY* format).
6. Delete the **RG1** resource group.

6.10.2 Results

6.11 After completing this exercise, you'll clean up the Azure resources that were created in the lab.

6.12 lab: title: 'Lab: Deploying and configuring Windows Server 2019 on Azure VMs' module: 'Module 6: Deploying and Configuring Azure VMs'

7 Lab: Deploying and configuring Windows Server 2019 on Azure VMs

7.1 Scenario

You need to address concerns regarding your current infrastructure. You have an outdated operational model, a limited use of automation, and Information Security team concerns regarding additional controls that should be applied to Azure VMs running Windows Server-based workloads. You have decided to develop and implement an automated deployment and configuration process for Azure VMs running Windows Server 2019.

The process will involve Azure Resource Manager (ARM) templates and OS configuration through Azure VM extensions. It will also incorporate additional security protection mechanisms beyond those already applied to on-premises systems, such as application whitelisting through AppLocker, file integrity checks, and adaptive network/DDoS protection. You will also leverage JIT functionality to restrict administrative access to Azure VMs to public IP address ranges associated with the London headquarters.

Your goal is to deploy and configure Azure VMs running Windows Server 2019 in the manner that satisfies manageability and security requirements.

7.2 Objectives

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

- Author ARM templates for an Azure VM deployment.
- Modify ARM templates to include VM extension-based configuration.
- Deploy Azure VMs running Windows Server 2019 by using ARM templates.
- Configure administrative access to Azure VMs running Windows Server 2019.
- Configure Windows Server 2019 security in Azure VMs.
- Deprovision the Azure environment.

7.3 Estimated time: 90 minutes

7.4 Lab setup

Lab virtual machines: **SEA-CL1** and **SEA-DC1**

User name: **CONTOSO\Administrator**

Password: **Pa55w.rd**

For this lab, you'll use the available VM environment and an Azure subscription. Before you begin the lab, ensure that you have an Azure subscription and a user account with the Owner or Contributor role in that subscription.

7.5 Exercise 1: Authoring ARM templates for Azure VM deployment

7.5.1 Scenario

To streamline Azure-based operations, you decide to develop and implement an automated deployment and configuration process for Windows Server 2019 to Azure VMs. Your deployments need to comply with the Information Security team's requirements and adhere to the Contoso, Ltd.'s intended target operational model, including high availability.

The main tasks for this exercise are as follows:

1. Enable the Standard tier of Security Center.
2. Generate an ARM template and parameters files by using the Azure portal.
3. Download the ARM template and parameters files from the Azure portal.

7.5.2 Task 1: Enable the Standard tier of Security Center

In this task, you will enable the Standard tier of Azure Security Center.

> **Note**: Skip this task and proceed directly to the next one if you have already upgraded Security Center in your Azure subscription to the Standard tier.

1. From **SEA-CL1**, start Microsoft Edge, and then navigate to the Azure portal. When prompted, sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
2. In the Azure portal, navigate to the **Security Center** blade.
3. From the **Security Center | Getting started** blade, upgrade Security Center to the Standard tier and select the option to automatically install the Security Center agents on all newly provisioned Azure VMs.

7.5.3 Task 2: Generate an ARM template and parameters files by using the Azure portal

1. From the Azure portal, go through the process of creating a new Azure VM using the following settings and leaving all other settings with their default values, but do not deploy it:

   Table 1: Azure VM settings

Setting	Value
Subscription	Use the name of the Azure subscription you will b
Resource group	The name of a new resource group ws2019-06-rg1
Virtual machine name	ws2019-06-vm0
Region	Use the name of an Azure region in which you can
Availability options	No infrastructure redundancy required
Image	Windows Server 2019 Datacenter-Gen1
Azure Spot instance	No
Size	Standard D2s v3
Username	Mike
Password	Pa55w.rd1234
Public inbound ports	None
Already have a Windows Server license	No
OS disk type	Standard HDD
Name	ws2019-06-vnet
Address range	10.60.0.0/20
Subnet name	subnet0

Setting	Value
Subnet range	10.60.0.0/24
Public IP	None
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Boot diagnostics	On
Diagnostics storage account	Use the default value.

2. When you reach the **Review + Create** tab of the **Create a virtual machine** blade, proceed to task 3.

7.5.4 Task 3: Download the ARM template and parameters files from the Azure portal

1. From the **Review + Create** tab of the **Create a virtual machine** blade, download the template for automation and copy it to the **C:\Labfiles\Mod06** folder on the lab VM.
2. In the Azure portal, close the **Create a virtual machine** blade.

7.6 Exercise 2: Modifying ARM templates to include VM extension-based configuration

7.6.1 Scenario

In addition to automated Azure resources deployments, you also want to ensure that you can automatically configure Windows Server 2019 OS's running in Azure VMs. To accomplish this, you want to test the use of Azure Custom Script Extension.

The main tasks for this exercise are as follows:

1. Review the ARM template and parameters files for Azure VM deployment.
2. Add an Azure VM extension section to the existing template.

7.6.2 Task 1: Review the ARM template and parameters files for Azure VM deployment

1. Extract the contents of the downloaded archive into the **C:\Labfiles\Mod06** folder.
2. Open the **template.json** file in Notepad and review the contents. Keep the Notepad window open.
3. Open the **C:\Labfiles\Mod06\parameters.json** file in Notepad, review it, and close the Notepad window.

7.6.3 Task 2: Add an Azure VM extension section to the existing template

1. On the lab VM, in the Notepad window displaying the contents of the **template.json** file, insert the following code directly underneath the `"resources": [` line):

```
{
   "type": "Microsoft.Compute/virtualMachines/extensions",
   "name": "[concat(parameters('virtualMachineName'), '/customScriptExtension')]",
   "apiVersion": "2018-06-01",
   "location": "[resourceGroup().location]",
   "dependsOn": [
       "[concat('Microsoft.Compute/virtualMachines/', parameters('virtualMachineName'))]"
   ],
   "properties": {
       "publisher": "Microsoft.Compute",
       "type": "CustomScriptExtension",
       "typeHandlerVersion": "1.7",
       "autoUpgradeMinorVersion": true,
       "settings": {
           "commandToExecute": "powershell.exe Install-WindowsFeature -name Web-Server -Inclu
      }
   }
},
```

2. Save the change and close the file.

7.7 Exercise 3: Deploying Azure VMs running Windows Server 2019 by using ARM templates

7.7.1 Scenario

With the ARM templates configured, you will verify their functionality by performing a deployment into your proof-of-concept Azure subscription.

The main tasks for this exercise are as follows:

1. Deploy an Azure VM by using an ARM template.
2. Review results of the Azure VM deployment.

7.7.2 Task 1: Deploy an Azure VM by using an ARM template

1. In the Azure portal, navigate to the **Custom deployment** blade and then select the option to **Build your own template in the editor**.
2. Load the template file and the parameter file into the **Custom deployment** blade.
3. Deploy the template with the following settings, leaving all other settings with their default values:

   Table 2: Custom template deployment settings

Setting	Value
Subscription	Use the name of the Azure subscription you are using in this lab.
Resource group	Use the resource group ws2019-06-rg1.
Region	Use the name of the Azure region into which you can provision Azure VMs.
Admin Password	Pa55w.rd1234

4. Verify that the deployment completed successfully.

   Note: The deployment might take about 10 minutes.

7.7.3 Task 2: Review results of the Azure VM deployment

1. In the Azure portal, navigate to the **ws2019-06-rg1** resource group blade and review the list of its resources, particularly the Azure VM **ws2019-06-vm0**.
2. Navigate to the **ws2019-06-vm0** Azure VM blade and verify that the **customScriptExtension** has been provisioned successfully.
3. Navigate back to the **ws2019-06-rg1** resource group blade, review its deployments, and review the **Microsoft.Template** that was used to deploy it to confirm that it matches the template you used for deployment.

7.8 Exercise 4: Configuring administrative access to Azure VMs running Windows Server 2019

7.8.1 Scenario

With the Azure VMs running Windows Server 2019 in place, you want to test the ability to manage them remotely from your on-premises administrative workstation.

The main tasks for this exercise are as follows:

1. Verify the Azure Security Center Standard tier.
2. Review Just in time VM access settings.

7.8.2 Task 1: Verify the Azure Security Center Standard tier

1. In the Azure portal, navigate to the **Security Center** blade.
2. Verify that the Standard tier for the **Security Center** is enabled.

7.8.3 Task 2: Review the Just in time access settings

1. In the **Security Center** blade, navigate to the **Just in time VM access settings**.
2. Review the **Unsupported** tab and verify that an entry representing the **ws2019-06-vm0** Azure VM appears on that tab.

   Note: It might take about 10 minutes for the VM to appear in the **Unsupported** tab. You may continue with the next exercise.

7.9 Exercise 5: Configuring Windows Server 2019 security in Azure VMs

7.9.1 Scenario

With the Azure VMs running Windows Server 2019 in place, you want to test the ability to manage them remotely from your on-premises administrative workstation.

The main tasks for this exercise are as follows:

1. Create and configure an NSG.
2. Configure inbound HTTP access to an Azure VM.
3. Configure inbound RDP access to the Azure VM.
4. Connect to the Azure VM via JIT VM access.

7.9.2 Task 1: Create and configure an NSG

1. In the Azure portal, create an NSG with the following settings, leaving all other settings with their default values:

   Table 3: Network security group settings

Setting	Value
Subscription	Use the name of the Azure subscription you are using in this lab.
Name	ws2019-06-vm0-nsg1
Resource group	ws2019-06-rg1
Region	Use the name of the Azure region into which you provisioned the Azure VM ws2019-06-vm0.

2. Add an inbound security rule to the newly created network security group with the following settings, leaving all other settings with their default values, and then select **Add**:

   Table 4: Network security group rule settings

Setting	Value
Source	Any
Source port ranges	*
Destination	Any
Destination port ranges	80
Protocol	TCP
Action	Allow
Priority	300
Name	AllowHTTPInBound

7.9.3 Task 2: Configure inbound HTTP access to an Azure VM

1. In the Azure portal, navigate to the blade of the network interface attached to the **ws2019-06-vm0** Azure VM, and associate it with the network security group you created in the previous task.
2. In the Azure portal, navigate to the IP configuration of the network interface attached to the **ws2019-06-vm0** Azure VM, and associate it with a new, public IP address with the following settings, leaving all others with their default values:

   Table 5: Public IP address settings

Setting	Value
Name	ws2019-06-vm0-pip1
SKU	Standard

3. From the lab VM, open a browser tab, navigate to the newly created public IP address, and verify that the page displays the message, **Hello World from ws2019-06-vm0**.
4. From the lab VM, attempt to establish a Remote Desktop connection to the same IP address and verify that the connection attempt fails.

   Note: This is expected behavior because the Azure VM is currently not accessible from the internet via TCP port 3389, only via TCP port 80.

7.9.4 Task 3: Trigger re-evaluation of the JIT status of an Azure VM

Note: This task is necessary to trigger re-evaluation of the JIT status of the Azure VM. By default, this might take up to 24 hours.

1. In the Azure portal, navigate back to the **Pricing** blade of **Azure Security Center** and switch to the **Free** tier by selecting **Azure Defender off** and **Save**.

   Note: Wait for about 2 minutes before you proceed to the next step.

2. In the Azure portal, navigate back to the **Security Center | Getting started** blade and switch back to the **Standard** tier by selecting **Upgrade** on the Upgrade tab and selecting **Install Agents**.
3. Refresh the browser window displaying the Azure portal.

7.9.5 Task 4: Configure inbound RDP access to the Azure VM

1. In the Azure portal, navigate to the **Security Center** blade.
2. In the **Security Center** blade, navigate to the **Just in time VM access settings**.
3. Review the **Not configured** tab, and verify that the entry representing the **ws2019-06-vm0** Azure VM is present on that tab.
4. Enable JIT VM access for the **ws2019-06-vm0** Azure VM.
5. Modify the **JIT VM access configuration** by removing access via TPC port 22.

   Note: It might take about 10 minutes for the VM to appear in the **Not configured** tab. To accelerate this process, select **Configuration** on the **ws2019-06-vm0** Azure VM and enable JIT VM access. Then select the link to **Open Azure Security Center**.

7.9.6 Task 5: Connect to the Azure VM via JIT VM access

1. From the **ws2019-06-vm0** blade in the Azure portal, request JIT VM access.
2. When the request is approved, initiate a Remote Desktop session to the target Azure VM.
3. When prompted for credentials, specify the following values, and then select **OK**:

   Table 6: Sign in credentials

Setting	Value
Username	Mike
Password	Pa55w.rd1234

4. Verify that you can successfully sign in to the Azure VM via Remote Desktop, and then close the Remote Desktop session.

7.10 Exercise 6: Deprovisioning the Azure environment

7.10.1 Scenario

To minimize Azure-related charges, you want to deprovision the Azure resources provisioned throughout this lab.

The main tasks for this exercise are as follows:

1. Start a PowerShell session in Cloud Shell.
2. Identify all Azure resources provisioned in the lab.

7.10.2 Task 1: Start a PowerShell session in Cloud Shell

1. From the Azure portal, open a PowerShell session in the **Azure Cloud Shell** blade.
2. If this is the first time you're starting **Cloud Shell**, accept the default settings.

7.10.3 Task 2: Identify all Azure resources provisioned in the lab

1. From the Cloud Shell blade, run the following command to list all resource groups created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-06-*'
   ```

2. From the Cloud Shell blade, run the following command to delete all the resource groups you created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-06-*'|Remove-AzResourceGroup -Force -AsJob
   ```

7.11 Results

After completing this lab, you will have deployed and configured Azure VMs running Windows Server 2019 in the manner that satisfies the Contoso, Ltd. manageability and security requirements.

7.11.1 Prepare for the next module

7.12 When you're finished with the lab, revert all virtual machines to their initial state. --- lab: title: 'Lab: Managing Azure VMs running Windows Server 2019' module: 'Module 7: Managing and maintaining Azure VMs'

8 Lab: Managing Azure VMs running Windows Server 2019

8.1 Lab scenario

To address concerns regarding the outdated operational model and Information Security concerns regarding additional controls that should be applied to Azure VMs running Windows Server-based workloads, you will test a new approach to management tasks that target Windows Server 2019 running in Azure VMs.

Rather than relying on Remote Desktop sessions—which are currently used for management of the on-premises computers running the Windows OS—for this purpose you will use a range of other tools at your disposal that streamline the running of management tasks.

8.2 Objectives

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

- Provision Azure VMs running Windows Server 2019.
- Manage Azure VMs running Windows Server 2019 by using Windows Admin Center.
- Manage Windows Server 2019 running in Azure VMs by using PowerShell Remoting.
- Manage Windows Server 2019 running in Azure VMs by using Run Command.
- Manage Windows Server 2019 in Azure VMs by using the serial console.
- Manage Windows Server 2019 in Azure VMs by using Azure Policy Guest Configuration.
- Deprovision the Azure lab environment.

8.3 Estimated time: 60 minutes

8.4 Lab setup

You'll need **WS-012T00A-SEA-DC1** and **WS-012T00A-SEA-CL1** to complete this lab.

Sign in to **SEA-CL1** as **Contoso\Administrator** by using **Pa55w.rd** as the password.

You will browse to the Azure portal from **SEA-CL1** and then use Azure VMs running Windows Server 2019 installed by using Azure PowerShell.

8.5 Exercise 1: Provisioning Azure VMs running Windows Server 2019

8.6 Scenario

You need to test a number of Azure VM management scenarios. To start, you will provision Azure VMs running Windows Server 2019 by using Azure PowerShell.

The main tasks for this exercise are to complete the following preparation steps:

1. Create a resource group.
2. Upload PowerShell scripts into Cloud Shell home directory.
3. Create two Azure VMs by using Azure Cloud Shell.

8.6.1 Task 1: Create a resource group

1. On **SEA-CL1**, start Microsoft Edge, navigate to the Azure portal, and sign in by using a user account with the Owner role in the Azure subscription you will be using in this lab.
2. In the Azure portal, create a resource group with the following settings:

   Table 1: Resource group settings

Setting	Value
Subscription	Use the name of the Azure subscription you will be using in this lab.
Resource group	ws2019-07-rg1
Region	Use the name of an Azure region in which you can provision Azure virtual machines.

8.6.2 Task 2: Upload PowerShell scripts into Cloud Shell home directory

1. On **SEA-CL1**, in the Microsoft Edge browser displaying the Azure portal, in a new browser tab, start a PowerShell session in the Cloud Shell. If prompted to authenticate, sign in by using a user account with the Owner role in the Azure subscription you are using in this lab.

   Note: If this is the first time you are starting **Cloud Shell**, use the default settings to configure it.

2. In the Cloud Shell tab, upload the following scripts from **C:\Labfiles\Mod07\Scripts**:

   - **Mod07Network.ps1**
   - **Mod07GW.ps1**
   - **Mod07TG.ps1**

8.6.3 Task 3: Create two Azure VMs by using Azure Cloud Shell

1. On **SEA-CL1**, in the Microsoft Edge browser displaying the Cloud Shell, from the PowerShell prompt, run the following command to create virtual network resources:

   ```
   ./Mod07Network.ps1
   ```

   Note: Ignore warnings regarding changes to PowerShell syntax.

2. In the Cloud Shell window, at the PowerShell prompt, run the following command to create the **Mod07Gateway** VM:

   ```
   ./Mod07GW.ps1
   ```

3. When prompted, authenticate by using the following credentials:

   Table 2: Mod07Gateway VM local Administrator credentials

Setting	Value
User	Student
Password	Pa55w.rd1234

   Note: It might take about 3-5 minutes to create the **Mod07Gateway** VM.

4. In the Cloud Shell window, at the PowerShell prompt, run the following command to create the

Mod07Target VM:

```
./Mod07TG.ps1
```

5. When prompted, authenticate by using the following credentials:

Table 3: Mod07Target VM local Administrator credentials

Setting	Value
User	Student
Password	Pa55w.rd1234

> **Note**: It might take approximately three to five minutes to create the **Mod07Target** VM.
>
> **Note**: Leave the Azure Cloud Shell tab open, because you'll use it later in this lab. After 20 minutes, the Cloud Shell will automatically disconnect, but you can select the **Reconnect** button to return to the PowerShell prompt.

8.7 Exercise 2: Managing Azure VMs running Windows Server 2019 by using Windows Admin Center

8.8 Scenario

To manage Azure VMs in a consistent manner, you'll install Windows Admin Center into an Azure VM and use it for common management tasks on another Azure VM.

The main tasks for this exercise are:

1. Install Microsoft Edge and Windows Admin Center on the Mod07Gateway Azure VM.
2. Add the Mod07Target VM to Windows Admin Center on Mod07Gateway VM.
3. Use Windows Admin Center to install the Web Server role on Mod07Target.

8.8.1 Task 1: Install Microsoft Edge and Windows Admin Center on the Mod07Gateway Azure VM

1. On **SEA-CL1**, in the Microsoft Edge window, from the Azure portal, connect to **Mod07Gateway** via Remote Desktop.
2. When prompted to authenticate, sign in as **Student** with the **Pa55w.rd1234** password.
3. Within the Remote Desktop session to **Mod07Gateway**, disable the **IE Enhanced Security Configuration** for Administrators.
4. Within the Remote Desktop session to **Mod07Gateway**, use Internet Explorer to download Microsoft Edge and install it with the default settings.

   > **Note**: The **Mod07Gateway** may be need time to apply Windows Updates before the Edge browser can be installed. Installing a Chrome browser can be a quicker option.
5. Within the Remote Desktop session to **Mod07Gateway**, use Microsoft Edge to download Windows Admin Center.
6. Within the Remote Desktop session to **Mod07Gateway**, install Windows Admin Center with the default settings.

8.8.2 Task 2: Add the Mod07Target VM to Windows Admin Center on Mod07Gateway VM

1. Within the Remote Desktop session to **Mod07Gateway**, use Microsoft Edge to access the locally installed Windows Admin Center instance at `https://Mod07Gateway`.
2. From **Windows Admin Center**, add a connection to **Mod07Target**.

8.8.3 Task 3: Use Windows Admin Center to install the Web Server role on Mod07Target

1. Within the Remote Desktop session to **Mod07Gateway**, in the Microsoft Edge browser, open a new tab and browse to `http://mod07target`. Note that the target page can't be reached. Keep the tab open and switch back to **Windows Admin Center**.
2. In **Windows Admin Center**, connect to **Mod07Target** and use the **Roles & features** feature to install on it the **Web Server (IIS)** server role and its services.

3. When the installation completes, switch to the Microsoft Edge tab targeting the `http://mod07target` URL and refresh the browser page. Verify that the browser displays the **Internet Information Services Welcome** page.
4. Switch back to **Windows AdminCenter** and, from the connection to **Mod07Target**, shut down its operating system.
5. Leave the Remote Desktop connection to **Mod07Gateway** open.

8.9 Exercise 3: Managing Windows Server 2019 running in Azure VMs by using PowerShell Remoting

8.10 Scenario

You must verify that you can perform scripted tasks targeting Azure VMs via PowerShell Remoting. For this purpose, you'll use Azure Cloud Shell.

The main tasks for this exercise are:

1. Configure PowerShell Remoting of an Azure VM running Windows Server 2019.
2. Manage Windows Server 2019 running in an Azure VM by using PowerShell Remoting.

8.10.1 Task 1: Configure PowerShell Remoting of an Azure VM running Windows Server 2019

1. On **SEA-CL1**, in the Microsoft Edge window, switch to Azure Cloud Shell. If needed, select **Reconnect**.
2. From the Cloud Shell blade, run the following commands to disable certificate verification for PowerShell remoting.

   ```
   install-module pswsman
   Disable-WSManCertVerification -All
   ```

3. In the Cloud Shell window, at the PowerShell prompt, run the following command to start the **Mod07Target** Azure VM:

   ```
   Start-AzVM -ResourceGroupName ws2019-07-rg1 -Name Mod07Target
   ```

4. After the VM successfully starts, in the Cloud Shell window, at the PowerShell prompt, run the following command to configure PowerShell Remoting on the **Mod07Target** Azure VM:

   ```
   Enable-AzVMPSRemoting -Name 'Mod07Target' -ResourceGroupName 'ws2019-07-rg1' -Protocol https -OsTy
   ```

   > **Note**: The **Enable-AzureVMPSRemoting** cmdlet configures WinRM on the target VM and configures its Network Security Group to allow access via Windows Remote Management.

8.10.2 Task 2: Manage Windows Server 2019 running in an Azure VM by using PowerShell Remoting

1. In the Cloud Shell window, at the PowerShell prompt, run the following command to list Windows services that have names that begin with **Win** installed within the operating system of the **Mod07Target** Azure VM:

   ```
   Invoke-AzVMCommand -Name 'Mod07Target' -ResourceGroupName 'ws2019-07-rg1' -ScriptBlock {get-servic
   ```

2. When prompted, authenticate as **Student** with the **Pa55w.rd1234** password.
3. Review the results displayed in the Cloud Shell pane and verify that they include a list of services that have names that begin with **Win**.
4. In the Cloud Shell window, at the PowerShell prompt, run the following command to start an interactive PowerShell Remoting session within the operating system of the **Mod07Target** Azure VM:

   ```
   Enter-AzVM -Name Mod07Target -ResourceGroupName ws2019-07-rg1 -Credential $Cred
   ```

5. When prompted, authenticate as **Student** with the **Pa55w.rd1234** password.

   > **Note**: You will be presented with an interactive session prompt. This allows you to run Windows PowerShell cmdlets directly against the target VM until you exit the session.

6. At the PowerShell Remoting session, run the following command to list locally installed Windows services that have names that begin with **Win**:

   ```
   Get-Service Win*
   ```

Note: The results should include the same list of services that you reviewed earlier in this task.

7. At the PowerShell Remoting session, run the following command to exit the interactive PowerShell Remoting session.

   ```
   Exit
   ```

8. Keep the **Cloud Shell** tab open.

8.11 Exercise 4: Managing Windows Server 2019 running in Azure VMs by using Run Command

8.12 Scenario

You want to explore the functionality of the Run command in the Azure portal for running simple commands targeting the Windows Server 2019 OS running in Azure VMs.

The main tasks for this exercise are:

1. Use the **EnableRemotePS** command.
2. Use the **RunPowerShellScript** command.

8.12.1 Task 1: Use the EnableRemotePS command

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, navigate to the **Mod07Target** blade.
2. From the **Mod07Target** blade, navigate to the **Mod07Target | Run command** blade.
3. From the **Mod07Target | Run command** blade, use the **EnableRemotePS** feature to enable PowerShell Remoting on the target operating system.
4. Wait until script execution completes.

8.12.2 Task 2: Use the RunPowerShellScript command

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, from the **Mod07Target | Run command** blade, use the **RunPowerShellScript** feature to run `Get-Service Win*` Windows PowerShell cmdlet.
2. Verify that the results include the same list of services that you reviewed in the previous task.
3. Close the **Run Command Script** blade.

8.13 Exercise 5: Managing Windows Server 2019 in Azure VMs by using the serial console

8.14 Scenario

You must ensure that you can recover the Windows Server 2019 OS running in an Azure VM, in case you can no longer access it using either RDP, the Run command, or PowerShell Remoting. To accomplish this, you'll test the Azure VM Serial console connection.

The main tasks for this exercise are:

1. Create a storage account.
2. Configure boot diagnostics for an Azure VM.
3. Use the serial console.

8.14.1 Task 1: Create a storage account

Note: Storage account names must be globally unique and can contain between 3 and 24 characters, including lowercase letters and numbers, starting with a letter.

1. On **SEA-CL1**, in the Microsoft Edge browser, in the Azure portal, navigate to the **Storage accounts** blade.

2. From the **Storage accounts** blade, create a storage account with the following settings (leave others with their default values):

   Table 4: Storage account settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-07-rg1
Storage account name	any globally unique name between 3 and 24 in length consisting of letters and digits
Location	the name of the Azure region where you created the resource group in the previous task
Performance	Standard
Account kind	Storage (general purpose v1)
Replication	Locally redundant storage (LRS)

Note: Wait for the Storage account to be created. This should take about two minutes.

8.14.2 Task 2: Configure boot diagnostics for an Azure VM

1. On **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, navigate to the **Mod07Target** Azure VM blade.
2. From the **Mod07Target** Azure VM blade, enable its boot diagnostics with the **Enable with custom storage account** option, using the storage account you created earlier in this exercise.

   Note: Managed storage account does not support the serial console functionality.

8.14.3 Task 3: Use the serial console

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, from the **Mod07Target** blade, activate the serial console.

   Note: The **Mod07Target | Serial console** blade should display the **SAC>** prompt
2. On the **Mod07Target | Serial console** blade, at the **SAC>** prompt, run **cmd** to create a channel that contains a CMD instance.
3. On the **Mod07Target | Serial console** blade, at the **SAC>** prompt, run **ch -si 1** to switch to the channel that's running the CMD instance.
4. On the **Mod07Target | Serial console** blade, select the Enter key, and then sign in with the following credentials:

   Table 5: Mod07Target VM local Administrator credentials

Setting	Value
User	Student
Domain	Mod07Target
Password	Pa55w.rd1234

5. On **Mod07Target | Serial console** blade, at the **C:\windows\system32** prompt, run the following to configure operating system boot options:

   ```
   bcdedit /set {bootmgr} displaybootmenu yes
   bcdedit /set {bootmgr} timeout 20
   bcdedit /set {bootmgr} bootems yes
   shutdown -r -t 0
   ```
6. On the **Mod07Target | Serial console** blade, when the EMS window displays, select the **F8** key to display the **Advanced Boot Option** screen.
7. On the **Mod07Target | Serial console** blade, within the serial console session, navigate the **Advanced Boot Option** screen and select the **Start Windows normally** option.
8. On the **Mod07Target | Serial console** blade, navigate back to the the **Mod07Target** blade.

   Note: The **Advanced Boot options** screen displays the message, **Choose Advanced Options for: Windows server 2016**. Mod07Target is running Windows Server 2019. This is expected, because the serial console code has not been updated on Windows Server 2019.

8.15 Exercise 6: Managing Windows Server 2019 in Azure VMs by using Azure Policy Guest Configuration

8.16 Scenario

You want to evaluate the capability of configuring Windows Server 2019 running in Azure VMs by using the Guest Configuration extension.

The main tasks for this exercise are:

1. Enable the Guest Configuration resource provider.
2. Assign an Azure Policy Guest Configuration by using the Azure portal.
3. Review results of the Guest Configuration policy.

8.16.1 Task 1: Enable the Guest Configuration resource provider

1. On **SEA-CL1**, in the Microsoft Edge window, switch to the tab displaying Azure Cloud Shell. If needed, select **Reconnect**.
2. In the Cloud Shell window, at the PowerShell prompt, run the following command to register the Guest Configuration resource provider:

   ```
   Register-AzResourceProvider -ProviderNamespace 'Microsoft.GuestConfiguration'
   ```

3. Wait until the resource provider is registered.

   Note: To verify the registration status, you can re-run the **Register-AzResourceProvider** cmdlet.

8.16.2 Task 2: Assign an Azure Policy Guest Configuration by using the Azure portal

1. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, navigate to the **Policy | Definitions** blade.
2. On the **Policy | Definitions** blade, locate the **Audit Windows machines on which the specified services are not installed and 'Running'** inititative definition.
3. From the **Policy | Definitions** blade, create an assignment of the **Audit Windows VMs on which the specified services are not installed and 'Running'** initiative definition with the following settings:

   Table 6: Initiative assignment settings

Setting	Value
Scope	**ws2019-07-rg1** resource group
Description	Auditing Windows services settings
Parameters (Service names)	W3SVC
Create remediation task	enabled with the default settings
Managed identity location	the same Azure region you used to deploy all Azure resources in this lab

   Note: **W3SVC** is the name of the World Wide Web Publishing Service, which you installed on **Mod07Target** earlier in this lab.

8.16.3 Task 3: Review results of the Guest Configuration policy

1. On **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, navigate back to the **Policy** blade.
2. On the **Policy** blade, note the **Audit Windows VMs on which the specified services are not installed and 'Running'** entry and verify that its **Compliance state** is listed as **Not started**
3. On **SEA-CL1**, in the Microsoft Edge window, switch to the tab displaying Azure Cloud Shell. If needed, select **Reconnect**.
4. In the Cloud Shell window, at the PowerShell prompt, run the following command to trigger an on-demand Azure Policy compliance scan targeting resources in the resource group **ws2019-07-rg1**:

   ```
   Start-AzPolicyComplianceScan -ResourceGroupName 'ws2019-07-rg1'
   ```

Note: Wait for the compliance scan to complete. For more information regarding time it takes to complete different types of Azure Policy processing, refer to Evaluation triggers and Validation frequency.

Note: Since you installed Web Server (IIS) server role on **Mod07Target**, that VM should be listed as compliant. However, since the resource group **ws2019-07-rg1** also contains the **Mod07Gateway** VM which does not include the Web Server (IIS) server role, the state of that resource and the assignment should be listed as **Non-compliant**.

5. To verify compliance status of individual resources, on **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, navigate to the **Mod07Target** blade.
6. From the **Mod07Target** blade, navigate to its **Policies** blade.
7. Verify that the **Audit Windows VMs on which the specified services are not installed and 'Running'** policy is listed as **Compliant**.
8. To verify compliance status of individual resources, on **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, navigate to the **Mod07Gateway** blade.
9. From the **Mod07Gateway** blade, navigate to its **Policies** blade.
10. Verify that the **Audit Windows VMs on which the specified services are not installed and 'Running'** policy is listed as **Non-compliant**.

8.17 Exercise 7: Deprovisioning the Azure lab environment

8.18 Scenario

To minimize Azure-related charges, you will deprovision the Azure resources provisioned throughout this lab.

The main tasks for this exercise are:

1. Remove the policy assignment.
2. Delete the ws2019-07-rg1 resource group.

8.18.1 Task 1: Remove the policy assignment

1. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, navigate to the **Policy** blade.
2. On the **Policy** blade, delete the **Audit Windows VMs on which the specified services are not installed and 'Running'** assignment.

8.18.2 Task 2: Delete the ws2019-07-rg1 resource group

1. In the Azure portal, navigate to the **ws2019-07-rg1** resource group blade.
2. From the **ws2019-07-rg1** resource group blade, delete the resource group.

8.19 Results

After completing this lab, you will have:

- Provisioned Azure VMs running Windows Server 2019.
- Managed Azure VMs running Windows Server 2019 by using Windows Admin Center.
- Managed Windows Server 2019 running in Azure VMs by using PowerShell Remoting.
- Managed Windows Server 2019 running in Azure VMs by using Run Command.
- Managed Windows Server 2019 in Azure VMs by using the serial console.
- Managed Windows Server 2019 in Azure VMs by using Azure Policy Guest Configuration.
- Deprovisioned the Azure lab environment. --- lab: title: 'Lab: Implementing Azure-based recovery services' module: 'Module 8: Planning and implementing migration and recovery services in hybrid scenarios'

---

9 Lab: Implementing Azure-based recovery services

9.1 Scenario

To address concerns regarding the outdated operational model, the limited use of automation, and reliance on tape backups for restores and disaster recovery, you decide to use Azure-based recovery services. As the first step, you'll implement Azure Site Recovery and Azure Backup.

9.2 Objectives

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

- Implement the lab environment.
- Create and configure an Azure Site Recovery vault.
- Implement Hyper-V VM protection by using Azure Site Recovery vault.
- Implement Azure Backup.
- Deprovision the Azure lab environment.

9.3 Estimated time: 60 minutes

9.4 Lab setup

Virtual machines: SEA-CL1 and SEA-DC1

User name: **Contoso\Administrator**

Password: **Pa55w.rd**

9.5 Exercise 1: Implementing the lab environment

9.5.1 Scenario

You need to test a number of Azure VM backup and recovery scenarios. To start, you will provision an Azure VM running Windows Server 2019 with the Hyper-V role installed by using an Azure Quickstart template. You will then install Hyper-V VM running Windows Server 2019 within that Azure VM.

The main tasks for this exercise are as follows:

1. Deploy an Azure VM running Windows Server 2019 with the Hyper-V role installed.
2. Connect to the Azure VM running the Windows Server 2019 with the Hyper-V role installed.
3. Download a Windows Server 2019 VHD file.
4. Deploy a Windows Server 2019 Hyper-V VM within an Azure VM.

9.5.1.1 Task 1: Deploy an Azure VM running Windows Server 2019 with the Hyper-V role installed

1. On **SEA-CL1**, start Microsoft Edge, navigate to the Azure portal, and sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
2. In the Azure portal, create a resource group with the following settings:

   Table 1: Resource group settings

Setting	Value
Subscription	Use the name of the Azure subscription you will be using in this lab.
Resource group	ws2019-08-rg1
Region	Use the name of an Azure region in which you can provision Azure virtual machines.

3. On **SEA-CL1**, open another Microsoft Edge tab, navigate to the 301-nested-vms-in-virtual-network Azure QuickStart template and use initiate a deployment the following settings:

   Table 2: QuickStart template deployment settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-08-rg1
Host Public IP Address Name	ws2019-08-hvm0-pip
Virtual Network Name	ws2019-08-hv-vnet
Host Network Interface1Name	ws2019-08-hvm0-nic1
Host Network Interface2Name	ws2019-08-hvm0-nic2
Host Virtual Machine Name	ws2019-08-hvm0
Host Admin Username	Student
Host Admin Password	Pa55w.rd1234

Note Wait for the deployment to complete. The deployment might take about 10 minutes.

9.5.1.2 Task 2: Connect to the Azure VM running the Windows Server 2019 with the Hyper-V role installed

1. On **SEA-CL1**, from the Microsoft Edge displaying the Azure Portal, navigate to the the **ws2019-08-hvm0 | Networking** blade.
2. From the **ws2019-08-hvm0 | Networking** blade, create an inbound port rule of the network security group associated with the **ws2019-08-hvm0-nic1** network adapter with the following settings:

   Table 3: Inbound security rule settings

Setting	Value
Destination port ranges	3389
Protocol	Any
Name	AllowRDPInBound

   Note Make sure that you modify the settings of **ws2019-08-hvm0-nic1**, which has the public IP address assigned to it.
3. In the Azure portal, navigate to the **ws2019-08-hvm0** blade.
4. From the **ws2019-08-hvm0** blade, connect via Remote Desktop to **ws2019-08-hvm0**. When prompted to authenticate, sign in as **Student** with the **Pa55w.rd1234** password.

9.5.1.3 Task 3: Download a Windows Server 2019 VHD file

1. Within the Remote Desktop session to **ws2019-08-hvm0**, from the **Server Manager** console, disable the **IE Enhanced Security Configuration** for Administrators.
2. Within the Remote Desktop session to **ws2019-08-hvm0**, use Internet Explorer to download a VHD file containing the **Windows Server 2019** evaluation image to the **F:\VHDs** folder from the Microsoft Evaluation Center web site.

9.5.1.4 Task 4: Deploy a Windows Server 2019 Hyper-V VM within an Azure VM

1. Within the Remote Desktop session to **ws2019-08-hvm0**, start **Hyper-V Manager**.
2. In the **Hyper-V Manager** console, create a new **Virtual Machine** with the following settings:

   Table 4: New virtual machine name and location settings

Setting	Value
Name	ws2019-08-vm1
Store the virtual machine in a different location	selected
Location	F:\VMs
Generation	Generation 1
Startup memory	2048
Use Dynamic Memory	enabled
Connection	NestedSwitch
Use an existing virtual hard disk	the VHD file you downloaded in the previous task

3. In the **Hyper-V Manager** console, connect to the newly provisioned Hyper-V VM and initialize the operating system with the default settings. When prompted, set the password of the built-in Administrator account to **Pa55w.rd1234**.
4. Sign in to the newly provisioned Hyper-V VM and run the following Windows PowerShell command to set the computer name:

```
Rename-Computer -NewName 'ws2019-08-vm1' -Restart
```

Note: The command will rename the operating system and restart it.

9.6 Exercise 2: Creating and configuring an Azure Site Recovery vault

9.6.1 Scenario

In order to implement Azure Site Recovery for the nested Windows Server 2019 VM running in an Azure VM, with Azure as the disaster recovery site, you have to first create and configure an Azure Site Recovery vault.

The main tasks for this exercise are as follows:

1. Create an Azure Site Recovery vault.
2. Configure the Azure Site Recovery vault.

9.6.1.1 Task 1: Create an Azure Site Recovery vault

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Internet Explorer window, navigate to the Azure portal, and sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
2. In the Azure portal, create a Recovery Services vault with the following settings (leave others with their default values):

Table 5: Recovery Services vault settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	the name of a new resource group ws2019-08-rg2
Vault name	ws2019-08a-rsvault
Location	the name of an Azure region different from the one into which you deployed the Azure VM in the first ex

Note By default, the default configuration for Storage Replication type is set to Geo-redundant (GRS) and Soft Delete is enabled. You will change these settings in the lab to simplify deprovisioning, but you should use them in your production environments.

9.6.1.2 Task 2: Configure the Azure Site Recovery vault

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, navigate to the **ws2019-08a-rsvault** blade.
2. From the **ws2019-08a-rsvault** blade, set **Storage replication type** of the vault to **Locally-redundant** which is in the Recovery Vault's Properties - Backup Configuration blade.

Note Storage replication type cannot be changed once you implement protection.

3. From the **ws2019-08a-rsvault** blade, disable **Soft Delete** of the vault which is in the Recovery Vault's Properties - Security Settings blade.

9.7 Exercise 3: Implementing Hyper-V VM protection by using Azure Site Recovery vault

9.7.1 Scenario

With a test Hyper-V VM and a Recovery Services vault created, you can now proceed to implement Hyper-V VM protection by using Azure Site Recovery. You will perform a test failover and review the settings of the planned and unplanned failover.

The main tasks for this exercise are as follows:

1. Implement an Azure recovery site.
2. Prepare protection of a Hyper-V virtual machine.
3. Enable replication of a Hyper-V virtual machine.
4. Review Azure VM replication settings.
5. Perform a failover of the Hyper-V virtual machine.

9.7.1.1 Task 1: Implement an Azure recovery site

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, create a virtual network with the following settings (leave others with their default values):

   Table 6: Virtual network ws2019-08-dr-vnet settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	the name of a new resource group ws2019-08-rg3
Name	ws2019-08-dr-vnet
Region	the name of the Azure region into which you deployed the Recovery Services vault earlier in this lab
IPv4 address space	10.8.0.0/22

2. Within the new virtual network, create a subnet with the following settings (leave others with their default values):

   Table 7: Virtual network ws2019-08-dr-vnet subnet subnet0 settings

Setting	Value
Subnet name	subnet0
Subnet address range	10.8.0.0/24

3. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, create another virtual network with the following settings (leave others with their default values):

   Table 8: Virtual network ws2019-08-test-vnet settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-08-rg3
Name	ws2019-08-test-vnet
Region	the name of the Azure region into which you deployed the Recovery Services vault earlier in this lab
IPv4 address space	10.0.0.0/22

4. Within the new virtual network, create a subnet with the following settings (leave others with their default values):

   Table 9: Virtual network ws2019-08-test-vnet subnet subnet3 settings

Setting	Value
Subnet name	subnet3
Subnet address range	10.0.2.0/24

   Note This matches the IP address range of the production network and the subnet containing the Hyper-V that needs to be protected.

5. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, create a storage account with the following settings (leave others with their default values):

   Table 10: Storage account settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-08-rg3
Storage account name	any globally unique name between 3 and 24 in length consisting of letters and digits, starting with
Location	the name of the Azure region into which you deployed the Recovery Services vault earlier in this la
Performance	Standard
Account kind	Storage (general purpose v1)
Replication	Locally redundant storage (LRS)

9.7.1.2 Task 2: Prepare protection of a Hyper-V virtual machine

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, navigate to the **ws2019-08a-rsvault** Recovery Services vault blade.
2. On the **ws2019-08a-rsvault** blade, in the vertical menu, start configuration of **Site Recovery**
3. On the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure** and specify the following settings:

   Table 11: Site Recovery Prepare infrastructure settings

Setting	Value
Deployment planning completed?	Yes, I have done it
Are you Using System Center VMM to manage Hyper-V hosts	No
Source setting: Hyper-V Site	ws2019-08 Hyper-V site

4. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V server** link.
5. On the **Add Server** blade, select the **Download** link in step 3 of the procedure for adding on-premises Hyper-V hosts in order to download the Microsoft Azure Site Recovery Provider.
6. Install **AzureSiteRecoveryProvider.exe** with **Microsoft Update** option disabled.
7. From the Azure portal, download the vault registration key into the **Downloads** folder.
8. Complete the **Provider installation** wizard and start the **Microsoft Azure Site Recovery Registration Wizard**.
9. When prompted, in the **Microsoft Azure Site Recovery Registration Wizard**, provide the location of the vault credentials file.
10. Complete the **Microsoft Azure Site Recovery Registration Wizard** with the default settings.
11. Refresh the browser page displaying the Azure portal and repeat the initial steps of the **1. Prepare infrastructure** procedure.
12. Once you reach the **Source settings** tab of the **Prepare infrastructure** blade, verify that the **Hyper-V site** and **Hyper-V servers** settings are set correctly and continue to the next step.
13. On the **Target settings** tab of the **Prepare infrastructure** blade, accept the default settings.
14. On the **Replication policy** tab of the **Prepare infrastructure** blade, create a new policy with the following settings and associate it with the the Hyper-V site:

    Table 12: Policy settings

Setting	Value
Name	ws2019-08 replication policy
Copy frequency	30 seconds

15. Complete the **Prepare infrastructure** procedure and wait until the association process completes

9.7.1.3 Task 3: Enable replication of a Hyper-V virtual machine

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, on the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **2. Enable replication**.
2. On the **Source environment** tab of the **Enable replication** blade, in the **Source location** drop-down list, select **ws2019-08 Hyper-V site**.
3. On the **Target environment** tab of the **Enable replication** blade, specify the following settings (leave others with their default values):

Table 13: Target environment settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Post-failover resource group	ws2019-08-rg3
Post-failover deployment model	Resource Manager
Storage account	the name of the storage account you created in the first task of this exercise
Azure network	Configure now for selected machines
Virtual network	ws2019-08-dr-vnet
Subnet	subnet0 (10.8.0.0/24)

4. On the **Virtual machine selection** tab of the **Enable replication** blade, select the **ws2019-08-vm1** entry.
5. On the **Replication settings** tab of the **Enable replication** blade, set the **Defaults** and **OS type** to **Windows**.
6. Complete the **Enable replication** procedure with the default settings.

9.7.1.4 Task 4: Review Azure VM replication settings

1. In the Azure portal, back on the **ws2019-08a-rsvault | Site Recovery** blade, in navigate to the the **ws2019-08a-rsvault | Replicated items** blade.
2. On the **ws2019-08a-rsvault | Replicated items** blade, ensure that there is an entry representing the **ws2019-08-vm1** virtual machine and verify that its **Replication Health** is listed as **Healthy** and that its **Status** is listed as either **Enabling protection** or displaying a current percentage of synchronization progress.

   Note You might need to wait a few minutes until the **ws2019-08-vm1** entry appears on the **ws2019-08a-rsvault | Replicated items** blade.
3. From the **ws2019-08a-rsvault | Replicated items** blade, navigate to the **ws2019-08-vm1** replicated items blade.
4. On the **ws2019-08-vm1** replicated items blade, review the **Health and status**, **Failover readiness**, **Latest recovery points**, and **Infrastructure view** sections. Note the **Planned Failover**, **Failover** and **Test Failover** toolbar icons.

   Note Wait until the status changes to **Protected**. This might take additional 15 minutes. You will need to refresh the browser page for the status to be updated. While waiting for the replication of the nested VM to complete, proceed to Exercise 4.
5. On the **ws2019-08-vm1** replicated items blade, select **Latest recovery points** and review **Latest crash-consistent** and **Latest app-consistent** recovery points.

9.7.1.5 Task 5: Perform a failover of the Hyper-V virtual machine

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the browser window displaying the Azure portal, on the **ws2019-08-vm1** replicated items blade, initiate **Test failover** with the following settings (leave others with their default values) and select **OK**:

Table 14: Test failover settings

Setting	Value
Choose a recovery point	the default option
Azure virtual network	ws2019-08-test-vnet

2. In the Azure portal, navigate back to the **ws2019-08a-rsvault** blade and, from there, navigate to the listing of **Site Recovery jobs**. Wait until the status of the **Test failover** job is listed as **Successful**.
3. In the Azure portal, navigate to the **Virtual machines** blade and note the entry representing the newly provisioned virtual machine **ws2019-08-vm1-test**.
4. In the Azure portal, navigate back to the **ws2019-08-vm1** replicated item blade and initiate **Cleanup test failover**.
5. Once the test failover cleanup job completes, refresh the browser page displaying the **ws2019-08-vm1** replicated items blade and note that you have the option to perform planned and unplanned failover.
6. From the **ws2019-08-vm1** replicated items blade, navigate to the **Planned failover** blade.
7. On the **Planned failover** blade, note that the failover direction settings are already set and not modifiable.
8. Close the **Planned failover** blade without initiating a failover.
9. From the **ws2019-08-vm1** replicated items blade, navigate to the **Failover** blade.
10. On the **Failover** blade, note that you have the option to choose a recovery point.
11. Close the **Failover** blade without initiating a failover.

9.8 Exercise 4: Implementing Azure Backup

9.8.1 Scenario

While waiting for the replication of the nested VM to complete, implement Azure Backup of the second Azure VM by using an Azure VM agent and Azure VM-level backup of the third Azure VM.

The main tasks for this exercise are as follows:

1. Create an Azure Site Recovery vault.
2. Configure the Azure Site Recovery vault.
3. Install the Azure Recovery Services agent.
4. Schedule Azure Backup.
5. Perform file recovery by using Azure Recovery Services agent.

9.8.1.1 Task 1: Create an Azure Site Recovery vault

Note While, in general, the same vault can be used to implement Azure Site Recovery and Azure Backup functionality, the one hosting Azure Backup should be located close to the location of the backed up items. For this reason, you will create another Azure Site Recovery vault in the same Azure region as the Azure VM you deployed in the second exercise of this lab.

1. Within the Remote Desktop session to **ws2019-08-hvm0**, switch to the Virtual Machine Connection window to **ws2019-08-vm1**.
2. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, from the **Server Manager** console, disable the **IE Enhanced Security Configuration** for Administrators.
3. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the Internet Explorer window, navigate to the Azure portal, and sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
4. In the Azure portal, create a Recovery Services vault with the following settings (leave others with their default values):

Table 15: Recovery Services vault settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	the name of a new resource group ws2019-08-rg4
Vault name	ws2019-08b-rsvault
Location	the name of an Azure region into which you deployed the Azure VM in the first exercise of this lab

Note By default, the default configuration for Storage Replication type is set to Geo-redundant (GRS) and Soft Delete is enabled. You will change these settings in the lab to simplify deprovisioning, but you should use them in your production environments.

9.8.1.2 Task 2: Configure the Azure Site Recovery vault

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the Azure portal, navigate to the **ws2019-08b-rsvault** blade.
2. From the **ws2019-08b-rsvault** blade, set **Storage replication type** of the vault to **Locally-redundant**.

   Note Storage replication type cannot be changed once you implement protection.
3. From the **ws2019-08b-rsvault** blade, disable **Soft Delete** of the vault.

9.8.2 Task 3: Install the Azure Recovery Services agent

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the Internet Explorer window displaying the Azure portal, on the **ws2019-08b-rsvault** Recovery Services vault blade, initiate **Backup** configuration with the following settings:

   Table 16: Backup settings

Settings	Value
Where is your workload running?	On-premises
What do you want to backup?	Files and folders

   Note Even though the virtual machine you are using in this task is running in Azure, you can leverage it to evaluate the backup capabilities applicable to any on-premises computer running Windows Server operating system.
2. From the **ws2019-08b-rsvault |Backup** blade, initiate the **Prepare infrastructure** procedure.
3. From the **Prepare infrastructure** blade, download Azure Recovery Services Agent, start the **Microsoft Azure Recovery Services Agent Setup Wizard**, disable the Microsoft Updates option, and complete the installation with the default settings.
4. After the installation completes, start the **Register Server Wizard**.
5. Switch to the Internet Explorer window displaying the Azure portal and, from the **Prepare infrastructure** blade, download the vault credentials file to the local Downloads folder.
6. Switch back to the **Register Server Wizard** window and, when prompted to provide Vault Credentials, point to the newly downloaded file.
7. On the **Encryption Setting** page of the **Register Server Wizard**, generate passphrase and store it in the local **Documents** folder.
8. Review the **Microsoft Azure Backup** warning and proceed to complete the registration. This will automatically open the **Microsoft Azure Backup** console.

   Note In a production environment, you should store the passphrase file in a secure location other than the server being backed up.

9.8.3 Task 4: Schedule Azure Backup

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the **Microsoft Azure Backup** console, schedule backup with the following settings (leave others with their default values):

Table 17: Scheduled backup settings

Settings	Value
Items to back up	C:\Windows\System32\drivers\etc\hosts
Backup Schedule	Daily at 4:30 AM
Retention Policy	default
Initial Backup type	default

2. In the **Microsoft Azure Backup** console, initiate an on-demand backup with the default settings.

   Note The option to run backup on demand becomes available once you create a scheduled backup.

3. Switch to the Internet Explorer window displaying the Azure portal, navigate back to the **ws2019-08b-rsvault** Recovery Services vault blade and display **Backup items**.
4. From the **ws2019-08b-rsvault | Backup items** blade, navigate to the **Backup Items (Azure Backup Agent)** blade and verify that there is an entry referencing the **C:** drive of **ws2019-08-vm1.**.

9.8.3.1 Task 5: Perform file recovery by using Azure Recovery Services agent

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, open File Explorer, navigate to the **C:\Windows\System32\drivers\etc** folder and delete the **hosts** file.
2. Switch to the Microsoft Azure Backup window and start **Recover Data Wizard** with the following settings (leave others with their default values):

   Table 18: Restore settings

Settings	Value
Restore target	This server (ws2019-08-vm1.)
Restore items	Individual files and folders
Select the volume	C:|

   Note Wait for the mount operation to complete. This might take about 2 minutes.

3. On the **Browse And Recover Files** page, note the drive letter of the recovery volume, select **Browse**, and review the tip regarding the use of **Robocopy**.
4. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, start **Command Prompt**.
5. From the **Administrator: Command Prompt** window, run the following to copy the restore the **hosts** file to the original location (replace `[recovery_volume]` with the drive letter of the recovery volume you identified earlier):

   ```
   robocopy [recovery_volume]:\Windows\System32\drivers\etc C:\Windows\system32\drivers\etc hosts /r:
   ```

6. From the **Administrator: Command Prompt** window, run the following to verify that the file has been restored:

   ```
   dir C:\Windows\system32\drivers\etc\hosts
   ```

7. Switch back to the **Recover Data Wizard** and unmount the mounted backup file.

9.9 Exercise 5: Deprovisioning the Azure lab environment

9.9.1 Scenario

To minimize Azure-related charges, you want to deprovision the Azure resources provisioned throughout this lab.

The main tasks for this exercise are as follows:

1. Remove the protected items.

2. Delete the lab resource groups.

9.9.2 Task 1: Remove the protected items

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, switch to the Internet Explorer window displaying the **Backup Items (Azure Backup Agent)** blade of the Azure portal and select the entry referencing the **C:** drive of **ws2019-08-vm1.**.
2. On the **C:\ on ws2019-08-vm1.** blade, navigate to the **ws2019-08-vm1.** blade.
3. From the **ws2019-08-vm1.** blade, specify the following information and delete the backup:

   Table 19: Backup item delete settings

Settings	Value
TYPE THE SERVER NAME	ws2019-08-vm1.
Reason	Decommissioned
Comments	Decommissioned

4. Close the Virtual Machine Connection window to **ws2019-08-vm1**, in the Remote Desktop session to **ws2019-08-hvm0**, in the Internet Explorer displaying the Azure portal, navigate to the **ws2019-08a-rsvault | Replicated items** blade, and select the **ws2019-08-vm1** entry.
5. From the **ws2019-08-vm1** replicated items blade, disable replication and remove remove replicated items without providing feedback.

9.9.3 Task 2: Delete the lab resource groups

1. On **SEA-CL1**, close the Remote Desktop session to **ws2019-08-hvm0**, switch to the Microsoft Edge window displaying the Azure portal.
2. In the Azure portal, open a PowerShell session in the **Azure Cloud Shell** pane.

   > **Note** If this is the first time you're starting **Cloud Shell** and you're presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and then select **Create storage**.

3. From the Cloud Shell blade, run the following command to delete all resource groups created in this lab:

```
Get-AzResourceGroup -Name 'ws2019-08-*' | Remove-AzResourceGroup -Force -AsJob
```

   > **Note** The command executes asynchronously (as determined by the *-AsJob* parameter), so while you will be able to run another PowerShell command immediately after within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.

9.10 lab: title: 'Lab: Implementing integration between AD DS and Azure AD' type: 'Answer Key' module: 'Module 2: Implementing Identity in Hybrid Scenarios'

10 Lab: Implementing integration between AD DS and Azure AD

10.1 Exercise 1: Preparing Azure AD for AD DS integration

10.1.1 Task 1: Create a custom domain in Azure

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Microsoft Azure portal.
2. Use the credentials that your instructor provides to sign in to the Azure portal.
3. In the Azure portal, browse to **Azure Active Directory**.
4. On the **Azure Active Directory** page, select **Custom domain names**.
5. On the **Custom domain names** page, select **Add custom domain**.

6. On the **Custom domain name** pane, in the **Custom domain name** text box, enter `contoso.com`, and then select **Add domain**.
7. On the `Contoso.com` custom domain name page, review the Domain Name System (DNS) record types that you would use to verify the domain.
8. Close the pane without verifying the domain name.

   Note: The domain name provided might not be a valid domain. While you would use DNS records to verify a domain, this lab doesn't require that verification step.

10.1.2 Task 2: Create a user with the Global Administrator role

1. On **SEA-SVR2**, on the **Azure Active Directory** page in the Azure portal, select **Users**.
2. On the **All Users** page, select **New User**.
3. On the **New User** page, under **Identity**, in the **User name** and **Name** text boxes, enter **admin**.

   Note: Ensure the domain name drop-down menu for the **User name** lists the default domain name ending with `onmicrosoft.com`.
4. Under **Password**, select the **Show Password** check box. Make note of the password as you'll use it later.
5. Under **Groups and roles**, next to **Roles**, select **User**.
6. On the **Directory roles** page, from the list of roles, select **Global administrator**, and then select **Select**.
7. On the **New user** page, select **Create**.

10.1.3 Task 3: Reset the password for the user with the Global Administrator role

1. On the Azure portal, select your user account, and then select **Sign out**.
2. On the **Pick an account** page, select **Use another account**.
3. On the **Sign in** page, enter the fully-qualified username of the user account you previously created, and then select **Next**.
4. For the current password, use the password that you wrote down in the previous step.
5. Enter **Pa55w.rdPa55w.rd** as the new password, and then select **Sign in**.

   Note: The Azure portal might not allow using the shorter password when updating.

10.2 Exercise 2: Preparing on-premises AD DS for Azure AD integration

10.2.1 Task 1: Install IdFix

1. On **SEA-SVR2**, open Microsoft Edge, and then browse to **https://github.com/microsoft/idfix**.
2. On the **Github** page, under **ClickOnce Launch**, select **launch**.
3. On the status bar, select **Open file**.
4. In the **Application Install - Security Warning** dialog box, select **Install**.
5. In the **IdFix Privacy Statement** dialog box, review the disclaimer, and then select **OK**.

10.2.2 Task 2: Run IdFix

1. In the **IdFix** window, select **Query**.
2. Review the list of objects from Active Directory, and observe the **ERROR** and **ATTRIBUTE** columns. In this scenario, the value of **displayName** for **ContosoAdmin** is blank, and the tool's recommended new value appears in the attribute column.
3. In the **IdFix** window, from the **ACTION** drop-down menu, select **Edit**, and then select **Apply** to automatically implement the recommended changes.
4. In the **Apply Pending** dialog box, select **Yes**.

5. Close the IdFix tool.

10.3 Exercise 3: Downloading, installing, and configuring Azure AD Connect

10.3.1 Task 1: Install and configure Azure AD Connect

1. On **SEA-SVR2**, open Microsoft Edge, browse to the Microsoft website, and search for "Install Azure AD Connect" to find the **Microsoft Azure Active Directory Connect** page.
2. On the **Microsoft Azure Active Directory Connect** page, select **Download**.
3. On the status bar, select **Open file**.
4. On the **Microsoft Azure Active Directory Connect** page, select the **I agree to the license terms and privacy notice** check box, and then select **Continue**.
5. On the **Express Settings** page, select **Use express settings**.
6. On the **Connect to Azure AD** page, enter the username and password of the Global Administrator account you created in exercise 1, then select **Next**.
7. On the **Connect to AD DS** page, enter the following credentials, and then select **Next**:
   - Username: **CONTOSO\Administrator**
   - Password: **Pa55w.rd**
8. On the **Azure AD sign-in configuration** page, verify that the new domain you added is in the list of Active Directory UPN Suffixes.

   Note: The domain name provided might not be a verified domain. While you typically must verify a domain prior to installing Azure AD Connect, this lab doesn't require that verification step.
9. Select the **Continue without matching all UPN suffixes to verified domains** check box, and then select **Next**.
10. On the **Ready to configure** page, review the list of actions, and then select **Install**.
11. On the **Configuration complete** page, select **Exit**.

10.4 Exercise 4: Verifying integration between AD DS and Azure AD

10.4.1 Task 1: Verify synchronization in the Azure portal

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Azure portal.
2. Sign in to the Azure portal by using the credentials for the account you created in exercise 1.
3. In the Azure portal, open **Azure Active Directory**.
4. On the **Azure Active Directory** page, select **Azure AD Connect**.
5. On the **Azure AD Connect** page, review the information under **Provision from Active Directory**.
6. On the **Azure Active Directory** page, select **Users**.
7. Observe the list of users that synced from the on-premises Active Directory.

   Note: When you begin directory synchronization, it can take 15 minutes for Active Directory objects to appear in the Azure AD portal.
8. In Microsoft Edge, select the **Back** button.
9. On the **Azure Active Directory** page, select **Groups**.
10. Observe the list of groups that synced from the on-premises Active Directory.

10.4.2 Task 2: Verify synchronization in the Synchronization Service Manager

1. On **SEA-SVR2**, on the **Start** menu, expand **Azure AD Connect**, and then select **Synchronization Service**.
2. In the **Synchronization Service Manager** window, under the **Operations** tab, observe the tasks that were performed to sync the Active Directory objects.

3. Select the **Connectors** tab and observe the two connectors.

   Note: One connector is for the on-premises Active Directory and the other is for the Azure domain.

4. Close the **Synchronization Service Manager** window.

10.4.3 Task 3: Update a user account in Active Directory

1. On **SEA-SVR2**, from **Server Manager**, open **Active Directory Users and Computers**.
2. In **Active Directory Users and Computers**, expand the **Sales** organizational unit (OU), and then open the properties for **Ben Miller**.
3. In the properties of the user, select the **Organization** tab.
4. In the **Job Title** text box, enter **Manager**, and then select **OK**.

10.4.4 Task 4: Create a user account in Active Directory

1. In **Active Directory Users and Computers**, right-click or access the context menu for the **Sales** OU, select **New**, and then select **User**.
2. In the **New Object - User** window, enter the following user details for each field, and then select **Next**:
   - First name: **Jordan**
   - Last name: **Mitchell**
   - User logon name: **Jordan**
3. In the **Password** and **Confirm password** fields, enter **Pa55w.rd**, and then select **Next**.
4. Select **Finish**.

10.4.5 Task 5: Sync changes to Azure AD

1. On **SEA-SVR2**, on the **Start** menu, select **Windows PowerShell**.
2. In the **Windows PowerShell** window, enter the following, and then select Enter:

   ```
   Start-ADSyncSyncCycle
   ```

   Note: When you begin directory synchronization, it can take 15 minutes for Active Directory objects to appear in the Azure AD portal

10.4.6 Task 6: Verify changes in Azure AD

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Azure portal.
2. On the **Azure Active Directory** page, select **Users**.
3. On the **All Users** page, search for the user **Ben**.
4. Open the properties page of the user **Ben Miller**, and then verify the **Job title** attribute that synced from Active Directory.
5. In Microsoft Edge, select the **Back** button.
6. On the **All Users** page, search for the user **Jordan**.
7. Open the properties page of the user **Jordan Mitchell**, and then verify the attributes that synced from Active Directory.
8. In Microsoft Edge, select the **Back** button twice.

10.5 Exercise 5: Implementing Azure AD integration features in AD DS

10.5.1 Task 1: Enable self-service password reset in Azure

1. On **SEA-SVR2**, in the Azure portal, on the **Azure Active Directory** page, select **Password reset**.
2. On the **Password reset** page, select **Get a free Premium trial to use this feature**.

3. On the **Activate** page, under **AZURE AD PREMIUM P2**, select **Free trial**, and then select **Activate**.
4. Right-click or access the context menu for the **Start** menu, select **Shut down or sign out**, and then select **Sign out**.
5. sign in to **SEA-SVR2** by using the following credentials:
   - Username: **CONTOSO\Administrator**
   - Password: **Pa55w.rd**
6. Start Microsoft Edge, and then browse to the Azure portal.
7. Sign in to the Azure portal by using the credentials of the account you created in exercise 1.
8. In the Azure portal, in the **Search resources, services, and docs** text box, enter **Azure Active Directory**, and then select **Azure Active Directory** from the drop-down menu.
9. On the **Azure Active Directory** page, select **Password reset**.
10. On the **Password reset** page, observe how you can select the scope of users to which to apply the configuration.

    Note: Don't enable the password reset feature because it will break the configuration steps that are required later in this lab.

10.5.2 Task 2: Enable password writeback in Azure AD Connect

1. On **SEA-SVR2**, open **Azure AD Connect**.
2. In the **Microsoft Azure Active Directory Connect** window, select **Configure**.
3. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter the username and password of the user account you created in exercise 1, and then select **Next**.
5. On the **Connect your directories** page, select **Next**.
6. On the **Domain and OU filtering** page, select **Next**.
7. On the **Optional features** page, select **Password writeback**, and then select **Next**.

   Note: Password writeback is required for self-service password reset. This allows passwords changed by users in Azure AD to sync to the on-premises Active Directory.
8. On the **Ready to configure** page, review the list of actions to be performed, and then select **Configure**.
9. On the **Configuration complete** page, select **Exit**.

10.5.3 Task 3: Enable pass-through authentication in Azure AD Connect

1. On **SEA-SVR2**, on the **Start** menu, expand **Azure AD Connect**, and then select **Azure AD Connect**.
2. In the **Microsoft Azure Active Directory Connect** window, select **Configure**.
3. On the **Additional tasks** page, select **Change user sign-in**, then select **Next**.
4. On the **Connect to Azure AD** page, enter the username and password of the user account you created in exercise 1, and then select **Next**.
5. On the **User sign-in** page, select **Pass-through authentication**.
6. Verify that the **Enable single sign-on** check box is selected, and then select **Next**.
7. On the **Enable single sign-on** page, select **Enter credentials**.
8. In the **Forest credentials** dialog box, enter the following credentials, and then select **OK**:
   - Username: **Administrator**
   - Password: **Pa55w.rd**
9. On the **Enable single sign-on** page, verify that there's a green check mark next to **Enter credentials**, and then select **Next**.

10. On the **Ready to configure** page, review the list of actions to be performed, and then select **Configure**.
11. On the **Configuration complete** page, select **Exit**.

10.5.4 Task 4: Verify pass-through authentication in Azure

1. On **SEA-SVR2**, on the **Azure Active Directory** page in the Azure portal, select **Azure AD Connect**.
2. On the **Azure AD Connect** page, review the information under **User Sign-In**.
3. Under **User Sign-In**, select **Seamless single sign-on**.
4. On the **Seamless single sign-on** page, review the on-premises domain name.
5. In Microsoft Edge, select the **Back** button to return to the previous page.
6. On the **Azure Active Directory** page in the Azure portal, select **Azure AD Connect**.
7. On the **Azure AD Connect** page, under **User Sign-In**, select **Pass-through authentication**.
8. On the **Pass-through authentication** page, review the list of servers under **Authentication Agent**.

   Note: To install the Azure AD Authentication Agent on multiple servers in your environment, you can open the **Azure AD Connect** page from the server, and then choose the **Download** option to install it on other servers.

10.5.5 Task 5: Install and register the Azure AD Password Protection proxy service and DC agent

1. On **SEA-SVR2**, start Microsoft Edge, and then browse to the Microsoft website, and search for "Azure AD Password Protection for Windows Server Active Directory" to find the **Azure AD Password Protection for Windows Server Active Directory** page, and select **Download**.
2. On **the Azure AD Password Protection for Windows Server Active Directory** page, select the AzureADPasswordProtectionProxySetup.exe and the AzureADPasswordProtectionDCAgentSetup.msi files, and then select **Next**.
3. Select **Download**.
4. In the **Download multiple files** dialog box, select **Allow**.

   Note: We recommend installing the proxy service on a server that isn't a domain controller.

5. On the status bar, locate the **AzureADPasswordProtectionProxySetup.exe** file, and then select **Open file**.
6. In the **Azure AD Password Protection Proxy Bundle Setup** window, select the **I agree to the license terms and conditions** check box, and then select **Install**.
7. In the **Installation Successfully Completed** window, select **Close**.
8. Open the **AzureADPasswordProtectionDCAgentSetup.msi** file to install the DC agent.
9. In the **Azure AD Password Protection DC Agent Setup** window, select the **I agree to the license terms and conditions** check box, and then select **Install**.
10. In the **Completed the Azure AD Password Protection DC Agent Setup Wizard** window, select **Finish**.
11. In the **Azure AD Password Protection DC Agent Setup** dialog box, select **No**.
12. On the **Start** menu, select **Windows PowerShell**.
13. In Windows PowerShell, enter the following command, and then select Enter:

    ```
    Get-Service AzureADPasswordProtectionProxy | fl
    ```

14. Verify that the status is **Running**.
15. To register the proxy service with Azure AD, enter the following command, and then select Enter:

    ```
    Register-AzureADPasswordProtectionProxy -AccountUpn <NewUser>
    ```

    Note: Replace <NewUser> with the fully-qualified user principal name of the account you created in exercise 1.

16. In the authentication window, enter the credentials for the account, and then select **Sign in**.
17. To register the proxy service with on-premises Active Directory, in Windows PowerShell, enter the following command, and then select Enter:

    ```
    Register-AzureADPasswordProtectionForest -AccountUpn <NewUser>
    ```

    Note: Replace <NewUser> with the fully-qualified user principal name of the account you created in exercise 1.

10.5.6 Task 6: Enable password protection in Azure

1. On **SEA-SVR2**, in the Azure portal, on the **Azure Active Directory** page, select **Security**.
2. On the **Security** page, select **Authentication methods**.
3. On the **Authentication methods** page, select **Password protection**.
4. On the **Password protection** page, change the slider for **Enforce custom list** to **Yes**.
5. In the **Custom banned password list** text box, enter the following words (one per line):
   - **Contoso**
   - **London**

   Note: The list of banned passwords should be words that are relevant to your organization.
6. Confirm the slider for **Enable password protection on Windows Server Active Directory** is set to **Yes**.
7. Confirm the slider for **Mode** is set to **Audit**, and then select **Save**.

10.6 Exercise 6: Cleaning up

10.6.1 Task 1: Uninstall Azure AD Connect

1. On **SEA-SVR2**, on the **Start** menu, select **Control Panel**.
2. In the **Control Panel** window, under **Programs**, select **Uninstall a program**.
3. In the **Uninstall or change a program** window, select **Microsoft Azure AD Connect**, and then select **Uninstall**.
4. In the **Programs and features** dialog box, select **Yes**.
5. In the **Uninstall Azure AD Connect** window, select **Remove**.
6. After the uninstall completes, in the **Uninstall Azure AD Connect** window, select **Exit**.

10.6.2 Task 2: Disable directory synchronization in Azure

1. On **SEA-SVR2**, on the **Start** menu, select **Windows PowerShell**.
2. To install the Microsoft Online module for Azure AD, in Windows PowerShell, enter the following command, and then select Enter:

   ```
   Install-Module -Name MSOnline
   ```
3. When prompted to install the NuGet provider, enter **Y**, and then select Enter.
4. When prompted to install the modules from an untrusted repository, enter **Y**, and then select Enter.
5. In Windows PowerShell, enter the following command to provide credentials to Azure, and then select Enter:

   ```
   $msolcred=Get-Credential
   ```
6. In the **Windows PowerShell credential request** dialog box, enter the credentials of the user account you created in exercise 1, and then select **OK**.
7. In Windows PowerShell, enter the following to connect to Azure, and then select Enter:

   ```
   Connect-MsolService -Credential $msolcred
   ```

8. In Windows PowerShell, enter the following to disable directory synchronization in Azure, and then select Enter:

```
Set-MsolDirSyncEnabled -EnableDirSync $false
```

9. When prompted to confirm, enter **Y**, and then select Enter.

10.7 lab: title: 'Lab: Using Windows Admin Center in hybrid scenarios' type: 'Answer Key' module: 'Module 3: Facilitating hybrid management and operational monitoring in hybrid scenarios'

11 Lab answer key: Using Windows Admin Center in hybrid scenarios

11.1 Exercise 1: Provisioning Azure VMs running Windows Server 2019

11.1.1 Task 1: Create an Azure resource group by using an Azure Resource Manager template

1. On SEA-CL1, start Microsoft Edge, navigate to the Azure portal, and sign in by using credentials of a user account with the Owner role in the subscription you'll be using in this lab.
2. In the Azure portal, open **Cloud Shell** blade by selecting on the toolbar icon directly next to the search textbox.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.

   Note: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and select **Create storage**.

4. In the toolbar of the Cloud Shell blade, select the **Upload/Download files** icon, in the drop-down menu select **Upload**, and upload the file **M03-lab-sub_template.json** into the Cloud Shell home directory, which can be found at C:\Labfiles\Mod03 into the Cloud Shell home directory.
5. From the Cloud Shell blade, run the following to create a resource group that will contain resources you provision in this lab Replace the `<Azure region>` placeholder with *eastus*:

```
$location = '<Azure region>'
New-AzSubscriptionDeployment `
  -Location $location `
  -Name ws2019-m031subDeployment `
  -TemplateFile $HOME/M03-lab-sub_template.json `
  -rgLocation $location `
  -rgName 'ws2019-m031-rg'
```

   Note: This lab has been tested and verified using East US, so you should use that region. In general, to identify Azure regions where you can provision Azure VMs, refer to Find Azure credit offers in your region.

11.1.2 Task 2: Create an Azure VM by using an Azure Resource Manager template

1. From the Cloud Shell blade, upload an Azure Resource Manager template **M03-lab-rg_template.json**, which can be found at C:\Labfiles\Mod03.
2. From the Cloud Shell blade, upload an Azure Resource Manager parameter file **M03-lab-rg_template.parameters.json**.
3. From the Cloud Shell blade, run the following to deploy a Azure VM running Windows Server 2019 that you'll be using in this lab:

```
New-AzResourceGroupDeployment `
  -Name ws2019-m031rgDeployment `
  -ResourceGroupName 'ws2019-m031-rg' `
  -TemplateFile $HOME/M03-lab-rg_template.json `
  -TemplateParameterFile $HOME/M03-lab-rg_template.parameters.json
```

Note: Wait for the deployment to complete before you proceed to the next exercise. The deployment should take less than 5 minutes.

4. In the Azure portal, close the **Cloud Shell** blade.
5. Review the **ws2019-m03-vnet** subnets. If there is no gateway subnet, then create a **Gateway subnet** using **10.3.3.224/27**.

11.2 Exercise 2: Implementing hybrid connectivity by using the Azure Network Adapter

11.2.1 Task 1: Register Windows Admin Center with Azure

1. On SEA-CL1, start Microsoft Edge and navigate to `https://sea-svr2.contoso.com` in order to connect to Windows Admin Center running on SEA-SVR2.
2. If prompted, sign in as **CONTOSO\Administrator** with **Pa55w.rd** as the password.
3. On the `https://sea-svr2.contoso.com` page in the Microsoft Edge, select the `sea-srv2.contoso.com [Gateway]` link.
4. On the Windows Admin Center page, select **Networks**, select **Actions**, and then select **+ Add Azure Network Adapter (Preview)**
5. When prompted, in the **Add Azure Network Adapter** window, select **Register Windows Admin Center to Azure**.

   Note: This will automatically display the **Azure** blade on the **Settings** page within the Windows Admin Center window.
6. On the **Azure** blade on the **Settings** page within the Windows Admin Center window, select **Register**.
7. On the **Get started with Azure in Windows Admin Center** blade, select **Copy** to copy the code displayed in step 1 of the registration procedure.
8. In step 2 of the registration procedure, select the link **Enter the code**.

   Note: This will open another tab in the Microsoft Edge window displaying the **Enter code** page.
9. In the **Enter code** text box, paste the code you copied into Clipboard and select **Next**.
10. On the **Sign in** page, provide the same user name that you used to sign into your Azure subscription in the previous exercise, select **Next**, provide the corresponding password, and select **Sign in**.
11. On the **Windows Admin Center** page verify that the sign in was successful and close the newly opened tab of the Microsoft Edge window.
12. Back on the **Get started with Azure in Windows Admin Center** blade, ensure that **Azure Active Directory application** is set to **Create new** and select **Connect**.
13. On the **Get started with Azure in Windows Admin Center** blade, in step 4, select the link **App Permissions in the Azure portal**.

    Note: This will open another tab in the Microsoft Edge window displaying the API permissions page of the **Windows Admin Center** app newly created in the Azure Active Directory tenant associated with your Azure subscription.
14. On the page of the **Windows Admin Center** app newly created in the Azure Active Directory tenant associated with your Azure subscription, select **Grant admin consent for Default Directory** and, when prompted for confirmation, select **Yes**.
15. Switch back to the Microsoft Edge tab displaying the **Get started with Azure in Windows Admin Center** blade and, in step 5 of the registration procedure, select the **Sign in** link.

11.2.2 Task 2: Create an Azure Network Adapter

1. In the Microsoft Edge tab, navigate back to the `sea-svr2.contoso.com` page and select **Networks** again.
2. On the Windows Admin Center page, in the **Networks** blade, select **+ Add Azure Network Adapter (Preview)**.

3. On the Add Network Adapter Settings blade, specify the following settings and select **Create** (leave others with their default values)"

Table 1: Azure Network Adapter settings

Setting	Value
Subscription	The name of the Azure subscription you are using in this lab
Location	eastus
Virtual network	ws2019-m03-vnet
Gateway subnet	10.3.3.224/27
Gateway SKU	VpnGw1
Client Address Space	192.168.0.0/24
Authentication Certificate	Auto-generated Self-signed root and client Certificate

4. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual network gateways**.
5. On the **Virtual network gateways** blade, select **Refresh** and verify that the new entry with the name starting with **WAC-Created-vpngw-** appears in the list of virtual network gateways.
6. On SEA-CL1, in the Microsoft Edge window displaying the Windows Admin Center running on SEA-SVR2, refresh the **Networks** blade and confirm that it displays the **WACVPN-26123** entry representing the Point-to-Site VPN connection with the IPv4 address of **192.168.0.1**.

   Note: The provisioning of the Azure virtual network gateway can take up to 45 minutes. Do not wait for the provisioning to complete but instead proceed to the next exercise.

11.3 Exercise 3: Deploying Windows Admin Center gateway in Azure

11.3.1 Task 1: Install Windows Admin Center gateway in Azure

1. On SEA-CL1, switch to the browser window displaying the the Azure portal.
2. Back in the Azure portal, open the **Azure Cloud Shell** blade by selecting by selecting the Cloud Shell button in the Azure Portal.
3. In the toolbar of the Cloud Shell blade, select the **Upload/Download files** icon, in the drop-down menu select **Upload**, and upload the file **Deploy-WACAzVM.ps1** into the Cloud Shell home directory.
4. From the Cloud Shell blade, run the following to enable the compatibility for the **AzureRm** PowerShell cmdlets that are used by the Windows Admin Center provisioning script:

   ```
   Enable-AzureRmAlias -Scope Process
   ```

5. From the Cloud Shell blade, run the following to set values of variables necessary to run the the Windows Admin Center provisioning script:

   ```
   $rgName = 'ws2019-m031-rg'
   $vnetName = 'ws2019-m03-vnet'
   $nsgName = 'ws2019-m03-web-nsg'
   $subnetName = 'subnet1'
   $location = 'eastus'
   $pipName = 'wac-public-ip'
   $size = 'Standard_D2s_v3'
   $image = 'Win2019Datacenter'
   ```

6. From the Cloud Shell blade, run the following to set the script parameters variable:

   ```
   $scriptParams = @{
     ResourceGroupName = $rgName
     Name = 'ws2019-wac-vm'
     VirtualNetworkName = $vnetName
     SubnetName = $subnetName
     GenerateSslCert = $true
     size = $size
     image = $image
   ```

```
}
```

7. From the Cloud Shell blade, run the following commands to disable certificate verification for PowerShell remoting.

```
install-module pswsman
Disable-WSManCertVerification -All
```

8. From the Cloud Shell blade, run the following to launch the provisioning script:

```
./Deploy-WACAzVM.ps1 @scriptParams
```

9. When prompted to provide the name for the local Administrator account, type **Student**
10. When prompted to provide the password for the local Administrator account, type **Pa55w.rd1234**

    Note: Wait for the provisioning script to complete. This might take about 5 minutes.

11. Verify that the script completed successfully and note the final message providing the URL containing the fully qualified name of the target Azure VM for the connection to the Windows Admin Center.
12. Close the Cloud Shell blade.

11.3.2 Task 2: Review results of the script provisioning

1. In the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Resource groups** and, on the **Resource groups** blade, select the **ws2019-m031-rg** entry.
2. On the **ws2019-m031-rg** blade, on the **Overview** blade, review the list of resources, including the Azure VM **ws2019-wac-vm**.
3. In the list of resources, select the Azure VM **ws2019-wac-vm** entry, and on the **ws2019-wac-vm** blade, select **Networking**.
4. On the **ws2019-wac-vm | Networking** blade, on the **Inbound port rules** tab, note entries representing the inbound port rule allowing connectivity on TCP port 5986 and the inbound rule allowing connectivity on TCP port 443.

11.4 Exercise 4: Verifying functionality of the Windows Admin Center gateway in Azure

11.4.1 Task 1: Connect to the Windows Admin Center gateway running in Azure VM

1. On SEA-CL1, start Microsoft Edge and navigate to the URL containing the fully qualified name of the target Azure VM hosting the Windows Admin Center gateway you identified in the previous exercise.
2. In Microsoft Edge window, disregard the message **Your connection isn't private**, select **Advanced**, and then select the link starting with the text **Continue to**.
3. When prompted, in the **Sign in to access this site** dialog box, provide the following credentials and select **OK**:

Table 2: Sign in credentials

Setting	Value
Username	Student
Password	Pa55w.rd1234

4. On the **All connections** blade of the Windows Admin Center page, select **ws2019-wac-vm [Gateway]**.
5. On the **Specify your credentials** blade, select the **Use another account for this connection** is selected, specify the following credentials, and select **Continue**.

Table 3: Sign in credentials

Setting	Value
Username	Student
Password	Pa55w.rd1234

6. Examine the **Overview** blade of the Windows Admin Center page.

11.4.2 Task 2: Enable PowerShell Remoting on an Azure VM

1. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual machines**.
2. On the **Virtual machines** blade, select **ws2019-m03-vm0**.
3. On the **ws2019-m03-vm0** blade, in the **Operations** section, select **Run command** and then select **RunPowerShellScript**.
4. On the **Run Command Script** blade, in the **PowerShell Script** section, type the following to and select **Run**:

   ```
   winrm quickconfig -quiet
   ```

5. On the **Run Command Script** blade, in the **PowerShell Script** section, replace the text you typed in the previous step with the following to and select **Run**:

   ```
   Set-NetFirewallRule -Name WINRM-HTTP-In-TCP-PUBLIC -RemoteAddress Any
   ```

6. On the **Run Command Script** blade, in the **PowerShell Script** section, replace the text you typed in the previous step with the following to and select **Run**:

   ```
   Enable-PSRemoting -Force -SkipNetworkProfileCheck
   ```

11.4.3 Task 3: Connect to an Azure VM by using the Windows Admin Center gateway running in Azure VM

1. On SEA-CL1, in the Microsoft Edge window displaying the interface of the Windows Admin Center gateway running on the **ws2019-wac-vm** Azure VM, select **Windows Admin Center**.
2. On the **All connections** page, select **+ Add**.
3. On the **Add or create resources** blade, in the **Servers** section, select **Add**.
4. In the **Server name** textbox, type **10.3.0.4** and select **Add**.
5. In the list of connections, select **10.3.0.4**
6. On the **Specify your credentials** blade, ensure the **Use another account for this connection** is selected, specify the following credentials, and select **Add with credentials**.

Table 4: Sign in credentials

Setting	Value
Username	Student
Password	Pa55w.rd1234

7. Once successfully connected, examine the **Overview** blade of the Windows Admin Center page on the second Azure VM with the IP address of **10.3.0.4**.

11.5 Exercise 5: Deprovisioning the Azure environment

11.5.1 Task 1: Start a PowerShell session in Cloud Shell

1. On SEA-CL1, switch to the Microsoft Edge window displaying the Azure portal.
2. In the Microsoft Edge window displaying the Azure portal, open the **Azure Cloud Shell** blade by selecting by selecting the Cloud Shell button in the Azure Portal.

11.5.2 Task 2: Identify all Azure resources provisioned in the lab

1. From the Cloud Shell blade, run the following to list all resource groups created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-m03*'
   ```

2. From the Cloud Shell blade, run the following to delete all resource groups you created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-m03*' | Remove-AzResourceGroup -Force -AsJob
   ```

   Note: The command executes asynchronously (as determined by the -AsJob parameter), so while you'll be able to run another PowerShell command immediately afterwards within the

same PowerShell session, it will take a few minutes before the resource groups are actually removed.

11.6 lab: title: 'Lab: Using Azure Security Center in hybrid scenarios' type: 'Answer Key' module: 'Module 4: Implementing Security Solutions in Hybrid Scenarios'

12 Lab: Using Azure Security Center in hybrid scenarios

12.1 Exercise 1: Provisioning Azure VMs running Windows Server 2019

12.1.1 Task 1: Start Azure Cloud Shell

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with password **Pa55w.rd**.
2. Open Microsoft Edge, and then browse to the Azure portal.
3. Sign in by using the credentials that you created for this course.
4. On the Azure portal, select **Cloud Shell**.
5. Select **PowerShell**.
6. When prompted, verify that your subscription is chosen, and then select **Create storage**.

12.1.2 Task 2: Create an Azure VM by using Azure Resource Manager templates

Upload the Resource Manager templates

1. In Cloud Shell, select **Upload/Download files**, and then select **Upload**.
2. Browse to the Desktop folder and then the **Allfiles\Labfiles\Mod04** folder.
3. Select the **M04-lab-rg_template.json** file, and then select **Open**.
4. Repeat steps 1 through 3 for the following files:
   - **M04-lab-rg_template.parameters.json**
   - **M04-lab-sub_template.json**

Create a resource group

1. In Cloud Shell, enter the following command, replacing *<region>* with an Azure region that's close to you:

   ```
   New-AzSubscriptionDeployment -Location '<region>' -Name ws2019-m04deployment -TemplateFile ./M04-la
   ```

Create a Windows Server virtual machine (VM)

1. In Cloud Shell, enter the following command:

   ```
   New-AzResourceGroupDeployment -Name windows-m04rgDeployment -ResourceGroupName m04-rg -TemplateFil
   ```

2. Close Cloud Shell.
3. Wait for deployment to complete.

   Note: You can close Cloud Shell before deployment is complete.

12.2 Exercise 2: Configuring Azure Security Center

12.2.1 Task 1: Make Security Center available and upgrade to the Standard pricing tier

1. Switch to Microsoft Edge, and then verify that you're signed in to the Azure portal.
2. In the search box, enter **Security Center**, and then select **Security Center** from the results.
3. On the **Security Center** menu, select **Getting started**.
4. On the **Upgrade** tab of the **Getting started** pane, for **Enable standard tier on 1 subscriptions**, select your subscription.
5. Select **Upgrade**.

   Note: Your subscription may already be upgraded for Security Center in which case there will not be an upgrade button and you may continue with Task 2.

6. Select **Continue without installing agents**.

12.2.2 Task 2: Turn on automatic provisioning of the Log Analytics agent

1. Browse back to Security Center.
2. In Security Center, select **Pricing & settings**, select your subscription, and then select **Auto Provisioning**.
3. In the **Log Analytics agent for Azure VMs** section, select **On** if it is not already enabled.
4. In the **Workspace configuration** section, verify that **ASC default workspace** is selected, and then select **Save** if it is not already enabled.
5. Refresh the page, and then browse back to the **Auto Provisioning** page.
6. Verify that **Log Analytics agent for Azure VMs** is **On** and the **Description** indicates that security related configurations and events will be collected. Select **Edit Configuration** and verify **All Events** is selected. If not, select it and save the setting.

   Note: It might take up to 30 minutes for the **Log Analytics** workspace to be created after selecting **Save** in step 4. You might need to refresh the page several times before the option to select **All Events** is available. Continue only after you're able to select **All events** and save the setting.

12.2.3 Task 3: Review the features and capabilities that apply to hybrid scenarios

1. In the **General** section of Security Center, select **Inventory**.
2. Review the **Recommendation** list.

   Note: The **Failed Resources** box indicates the type of resource to which the recommendation applies and lists how many resources the recommendation applies to.
3. Under the **Resource Name** column select the **ws2019-m04-vm0** VM.
4. Note the details of the VM's security health.
5. Close the **ws2019-m04-vm0** pane.
6. In the **Coud Security** section, select **Regulatory compliance**.
7. Under **Azure Security Benchmark**, select **expand all compliance controls**, and then review the assessments.

12.3 Exercise 3: Onboarding on-premises Windows Server 2019 into Azure Security Center

12.3.1 Task 1: Download and install the Log Analytics agent

1. On **SEA-CL1**, switch to Microsoft Edge, and then verify that you're signed in to the Azure portal.
2. In the search box, enter **Log Analytics**, and then select **Log Analytics workspaces** from the results.
3. Select the listed Log Analytics workspace. There should only be one, and the name will start with "DefaultWorkspace".
4. Select **Agents management**.
5. Copy and save the **WORKSPACE ID** and the **PRIMARY KEY**.

   Note: You can save these values in Notepad or make a note of them.
6. Select the **Download Windows Agent (64 bit)** link.
7. In the download status bar, on the context menu for **MMASetup-AMD64.exe**, select **Show in folder**.
8. Copy the file to **c:\labfiles\mod04**. Create the folder if needed.
9. Select **Start**, and then open Windows PowerShell.
10. In PowerShell, browse to **c:\labfiles\Mod04**.
11. Enter the following command:

```
.\MMASetup-amd64.exe /c /t:c:\labfiles\mod04
```

12. Open a new tab in Microsoft Edge, open **Windows Admin Center**, and then sign in as **Administrator** with password **Pa55w.rd**.
13. Select **Add**.
14. Under **Windows Server**, select **Add**.
15. Under **Server name**, enter `sea-svr1.contoso.com`, and then select **Add**.
16. In **Windows Admin Center**, select **SEA-SVR1**, and then sign in as **Contoso\Administrator** with password **Pa55w.rd**.
17. Select SEA-SVR1, select **PowerShell**, and then enter the password **Pa55w.rd**.
18. Enter the following commands:

```
mkdir c:\labfiles\mod04
copy \\SEA-CL1\c$\labfiles\mod04\*.* c:\labfiles\mod04\
```

19. Browse to **c:\labfiles\mod04**.
20. Enter the following command:

```
.\setup.exe /qn NOAPM=1 ADD_OPINSIGHTS_WORKSPACE=1 OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIG
```

    where *<workspaceID>* is the WORKSPACE ID that you copied earlier and *<primarykey>* is the PRIMARY KEY that you copied earlier.
21. Wait for the installation to complete.

12.4 Exercise 4: Verifying the hybrid capabilities of Azure Security Center

12.4.1 Task 1: Validate the Security Center capabilities for Azure VMs

1. Open Microsoft Edge, and then browse to the Azure portal.
2. Sign in by using the credentials that you created for this course.
3. In the search box, enter **Virtual Machines**, and then select **Virtual Machines** from the results.
4. Select the **ws2019-m04-vm0** VM.
5. Select **Connect**, select **RDP**, and then select **Download RDP File**.
6. In the download status bar, select the context menu for the **ws2019-mo4-vm0.rdp** file, and then select **Open**.
7. If prompted, select **Connect**.
8. Enter the username **Student** with password **Pa55w.rd1234**.
9. In the VM's Remote Desktop session, select **Start**, and then select **Windows PowerShell**.
10. Enter the following commands:

```
mkdir c:\temp
powershell -nop -exec bypass -EncodedCommand "cABvAHcAZQByAHMAaABlAGwAbAAgACOAYwBvAGOAbQBhAG4AZAAg
```

11. In Microsoft Edge, switch to the Azure portal tab.
12. In the search box, enter **Security Center**, and then select **Security Center** from the results.
13. On the **Overview** page, review the **Threat protection** section. You should have one new alert. If not, wait a few minutes.
14. In the **General** section of the **Security Center** menu, select **Security alerts**. There should be one alert.
15. In the **General** section of the **Security Center** menu, select **Inventory**.
16. Select the **ws2019-mo4-vm0** VM.
17. Review the recommendations.

12.4.2 Task 2: Validate the Security Center capabilities for on-premises VMs

1. In Microsoft Edge, switch to the **Windows Admin Center** tab.
2. Verify that you're signed in to **SEA-SVR1** as **Contoso\Administrator**, and then select **PowerShell**.
3. Enter the following commands:

   ```
   mkdir c:\temp
   powershell -nop -exec bypass -EncodedCommand "cABvAHcAZQByAHMAaABlAGwAbAAgACOAYwBvAGOAbQBhAG4AZAAg
   ```

4. Open Microsoft Edge, and then browse to the Azure portal.
5. Sign in by using the credentials that you created for this course.
6. In the search box, enter **Security Center**, and then select **Security Center** from the results.
7. On the **Overview** page, review the **Azure defender** section. You should have one new alert for **SEA-SVR1**. If not, wait a few minutes.
8. In the **General** section of the **Security Center** menu, select **Security alerts**. There should be a new alert for **SEA-SVR1**.
9. In the **General** section of the **Security Center**, select **Inventory** and then select **SEA-SVR1**.
10. Review the recommendations for **SEA-SVR1**.

    Note: You might need to wait several minutes for **SEA-SVR1** to be listed.

12.5 Exercise 5: Deprovisioning the Azure environment

12.5.1 Task 1: Start a PowerShell session in Cloud Shell

1. On **SEA-CL1**, in Microsoft Edge, switch to the Azure portal.
2. Select **Cloud Shell**.

12.5.2 Task 2: Identify and remove all Azure resources that were provisioned in the lab

- In Cloud Shell, enter the following command to find and remove all resource groups:

  ```
  Get-AzResourceGroup | Remove-AzResourceGroup -Force
  ```

12.5.3 Task 3: Prepare for the next module

- End the lab.

12.6 lab: title: 'Lab: Implementing Azure File Sync' type: 'Answer Key' module: 'Module 5: Implementing File Services in Hybrid Scenarios'

13 Lab: Implementing Azure File Sync

13.1 Exercise 1: Implementing Distributed File System (DFS) Replication in your on-premises environment

13.1.1 Task 1: Deploy DFS

1. Sign in to **SEA-CL1** as **Contoso\Administrator** and use **Pa55w.rd** as the password.
2. On the taskbar, select **File Explorer**. If in the Lab Setup the **Allfiles** folder was copied to the **Desktop**, then open the **Allfiles** folder, and copy the **Labfiles** folder to **C:**. Then share the **Labfiles** folder to **Everyone** with **Read** access.
3. In File Explorer, browse to the **C:\Labfiles\Mod05** folder.
4. In File Explorer, in the **details** pane, right-click or access the context menu for **M05_DeployDFS.ps1**, and then select **Run with PowerShell**.

13.1.2 Task 2: Test DFS deployment

1. On **SEA-CL1**, select **Start**, enter **DFS**, and then select **DFS Management**.
2. In **DFS Management**, in the **navigation** pane, right-click or access the context menu for **Namespaces**, and then select **Add Namespaces to Display**.
3. In the **Add Namespaces to Display** dialog box, ensure that `\\Contoso.com\Root` is selected in **Namespaces** section, and then select **OK**.
4. In the **navigation** pane, right-click or access the context menu for **Replication**, and then select **Add Replication Groups to Display**.
5. In **Add Replication Groups to Display** dialog box, in **Replication Groups** section, select **Branch1**, and then select **OK**.
6. In the **navigation** pane, expand the `\\Contoso.com\Root` namespace, and then select the **Data** folder.
7. In the **details** pane, verify that the **Data** folder has two referrals, on **LON-SVR1** and **SEA-SVR1**.
8. In the **navigation** pane, select **Branch1**.
9. In the **details** pane, verify that the **D:\Data** folder on **LON-SVR1** and on **SEA-SVR1** are members of the **Branch1** replication group.

   Note: DFS Replication replicates the content between the **D:\Data** folders on **LON-SR1** and **SEA-SVR1**.
10. Open two instances of File Explorer. In the first File Explorer instance, connect to **\\LON-SVR1\Data**, and then in the second File Explorer instance, connect to **\\SEA-SVR1\Data**.

    Note: Wait until the files are replicated and both the File Explorer windows record the same content.
11. Create a new file with your name in **\\LON-SVR1\Data**.
12. Verify that the file with your name replicates to **\\SEA-SVR1\Data** after a few seconds. This confirms that DFS Replication is working.

13.2 Exercise 2: Creating and configuring a sync group

13.2.1 Task 1: Create an Azure file share

1. On **SEA-CL1**, select **Microsoft Edge** on the taskbar.
2. In Microsoft Edge, open the Azure portal, and then authenticate with your Azure credentials.
3. In the Azure portal, select **Storage accounts**, and then select **Add**.
4. Create a storage account by using following settings:
   - Resource group: Select **Create new**, enter **RG1** as resource group name, and then select **OK**.
   - Storage account name: All letters in the name must be lowercase, and the name must be unique. For example, you can specify the storage account name in the following format: *<YourLowercaseInitials>DDMMYY*; for example, **dt150620** if your name is Devon Torres and you're creating a storage account on June 15, 2020. If that name is already taken, add another character to the name until the name is available. Accept the default values for all other settings, select **Review create**, and then select **Create**.

     Note: Use the same region for deploying all resources in this lab.
5. After the storage account is created, select **Go to resource**.
6. On the **storage account** blade, select **File shares**, and then select **File share**.
7. On the **New file share** tab, enter **share1** in the **Name** text box, and then select **Create**.

13.2.2 Task 2: Use an Azure file share

1. On **SEA-CL1**, in the Azure portal, in the **details** pane, select **share1**.
2. In the **details** pane, select **Upload**.

3. On the **Upload files** tab, browse to **C:\Labfiles\Mod05\File1.txt**, select **Upload**, and when the upload is complete, close the **Upload files** tab.
4. On the **share1** blade, select **Snapshots**, select **Add snapshot**, and then select **OK**.
5. On the **share1** blade, select **Overview**, select **Connect**, use the **Copy to clipboard** button to copy the script, and then close the **Connect** tab.
6. Right-click or access the context menu for **Start**, and then select **Windows PowerShell**.
7. Right-click or access the context menu for the **Windows PowerShell** window to paste the text from the Clipboard. Select Enter to continue the script.

   Note: The script mounted the Azure file share to drive letter **Z**.
8. On the taskbar, right-click or access the context menu for **File Explorer**, select **File Explorer**, and then in the **navigation** pane, select **share1**.
9. Verify that you can observe **File1.txt** in the **details** pane. This is the file that you uploaded to the Azure file share.
10. Double-click or select **File1.txt**, and then select Enter. Change the file by entering your name, close Notepad, and then save the changes.
11. Right-click or access the context menu for **File1**, select **Properties**, and then select the **Previous Versions** tab.
12. Verify that one previous file version is available. Select that version (**File1.txt**), select **Restore** twice, and then select **OK** twice.
13. Double-click or select **File1.txt**, select Enter, and then confirm that it doesn't include your name. This is because you created the snapshot before you modified the file.
14. Close **Notepad**.

13.2.3 Task 3: Deploy Storage Sync Service and a File Sync group

1. On **SEA-CL1**, in the Azure portal, select **Create a resource** on the **navigation** blade, enter **Azure File Sync** in the text box, select **Azure File Sync**, and then select **Create**.
2. In the **Deploy File Sync** pane, for **Resource Group**, select **RG1**. Enter **FileSync1** as the Storage Sync Service name, ensure that the same region is selected as was used for the storage account, and then select **Review and create** and **Create**.
3. After Storage Sync Service deploys, select **Go to resource**.
4. On the **Storage Sync Service** blade, select **Sync groups**, and then select **Sync group** to create a new File Sync group.
5. In the **Sync group** pane, enter **Sync1** in the **Sync group name** text box.
6. Select **Select storage account**, and then select the storage account that you created. If you can't find the storage account, it was probably deployed to a different Azure region. You must deploy a new Azure storage account in such a case.
7. In the **Azure File Share** drop-down list, select **share1**, and then select **Create**.
8. On the **Storage Sync Service** blade, select **Registered servers**, and then confirm that no server is currently registered.

13.3 Exercise 3: Replacing DFS Replication with File Sync-based replication

13.3.1 Task 1: Add SEA-SVR1 as a server endpoint

1. On **SEA-CL1**, in the Azure portal, download the File Sync agent for Windows Server 2019 (**StorageSyncAgent_WS2019.msi**), and then save it to the **C:\Labfiles** folder. After the download is complete, close the Microsoft Edge tab that opened for the download.

   Note: If you downloaded the file to the default location, you need to copy the file to the **C:\Labfiles** folder.
2. In File Explorer, browse to the **C:\Labfiles\Mod05** folder, and then double-click or select **InstallFileSyncServerCore.ps1**.

3. In Notepad, update the value of the *$RG_name* variable with the name of the resource group to which you deployed **FileSync1** (replace everything inside <>, including < and >, but leave the apostrophe at the beginning and at the end), and then save the file.
4. Right-click or access the context menu for **Start**, select **Windows PowerShell**, enter **cd C:\Labfiles\Mod05**, and then select Enter.
5. Enter **.\Install-FileSyncServerCore.ps1**, and then select Enter.
6. Wait while the script runs—it takes some time. When you get the **WARNING** output, copy the nine-character code in the warning output to the Clipboard.
7. Open a new tab in Microsoft Edge by selecting +, and then browse to **https://microsoft.com/devicelogin**.
8. In Microsoft Edge, paste the code in the **Enter code** dialog box, sign in with your Azure credentials, and then close the Microsoft Edge tab that you opened in the previous step.
9. When the script finishes, refresh the list of registered servers in the Azure portal by selecting **Refresh**.
10. Confirm that the `SEA-SVR1.Contoso.com` server is now registered in the **FileSync1** Storage Sync Service.
11. In File Explorer, open **\\SEA-SVR1\Data**, and then verify that the folder doesn't contain **File1.txt**.
12. In the Azure portal, on the **Storage Sync Service** blade, select **Sync Groups**, select **Sync1**, and then select **Add server endpoint**.
13. On the **Add server endpoint** tab, select `SEA-SVR1.Contoso.com` in the **Registered servers** list.
14. In the **Path** text box, enter **D:\Data**, and then select **Create**.
15. In the File Explorer that has the **\\SEA-SVR1\Data** folder open, verify that **File1.txt** is present.

    Note: You uploaded **File1.txt** to the Azure file share, from where it was synced to **SEA-SVR1** by File Sync.

13.3.2 Task 2: Register LON-SVR1 with File Sync

1. On **SEA-CL1**, in File Explorer, double-click or select **Install-FileSyncServerCore.ps1** in the **C:\Labfiles\Mod05** folder, and then select Enter.
2. In Notepad, for the *$Server* variable, replace **SEA-SVR1** with **LON-SVR1**, and then save the file.
3. On the taskbar, select **Windows PowerShell**, enter **.\Install-FileSyncServerCore.ps1**, and then select Enter.
4. Wait while the script runs—it takes some time. When you get the **WARNING** output, copy the nine-character code in the warning output to the Clipboard.
5. In Microsoft Edge, open a new tab by selecting +, and then browse to **https://microsoft.com/devicelogin**.
6. In Microsoft Edge, paste the code in the **Enter code** dialog box, sign in with your Azure credentials, and then close the Microsoft Edge tab that you opened in the previous step.
7. When the script finishes, in the Azure portal, select **Registered servers** on the **FileSync1** blade.
8. Confirm that `SEA-SVR1.Contoso.com` and `LON-SVR1.Contoso.com` are registered with the **FileSync1** Storage Sync Service.

13.3.3 Task 3: Remove DFS Replication and add LON-SVR1 as a server endpoint

1. On **SEA-CL1**, select **DFS Management** on the taskbar.
2. In **DFS Management**, in the **navigation** pane, right-click or access the context menu for **Branch1**, select **Delete**, select the **Yes, delete the replication group, stop replicating all associated replicated folders, and delete all members of the replication group** option, and then select **OK**.
3. In the Microsoft Edge tab that has the Azure portal open, select **Sync Groups**, select **Sync1**, and then select **Add server endpoint**.
4. On the **Add server endpoint** tab, select `LON-SVR1.Contoso.com` in the **Registered servers** list, enter **D:\Data** in the **Path** text box, and then select **Create**.

13.4 Exercise 4: Verifying replication and enabling cloud tiering

13.4.1 Task 1: Verify File Sync

1. On **SEA-CL1**, use two instances of File Explorer. In the first File Explorer instance, connect to **\\LON-SVR1\Data**, and then in the second File Explorer instance, connect to **\\SEA-SVR1\Data**.

2. Create a file with your last name in the **\\LON-SVR1\Data** folder.
3. Verify that after some time, the file with your last name also appears in the **\\SEA-SVR1\Data** folder.

   Note You removed DFS Replication in the previous exercise. File Sync replicated the file with your name.

13.4.2 Task 2: Enable cloud tiering

1. On **SEA-CL1**, in the Azure portal, browse to the **Sync1** sync group in the **FileSync1** Storage Sync Service.
2. In the Azure portal, select `LON-SVR1.Contoso.com` in the **Server endpoint** section.
3. On the **Server Endpoint Properties** tab, select **Enabled** in the **Cloud Tiering** section.
4. In the **Always preserve the specified percentage of free space on the volume** text box, enter **90**, select **Enabled** for the **date policy**. In the **Only cache files that were accessed or modified within the specified number of days** text box, enter **14**, and then select **Save**.

   Note: After some time, files on **LON-SVR1** would automatically tier. You can trigger tiering immediately by running on LON-Cl1:

```
Enter-PSSession -computername lon-svr1
Import-Module "C:\Program Files\Azure\StorageSyncAgent\StorageSync.Management.ServerCmdlets.dll"
Invoke-StorageSyncCloudTiering -Path D:\data
```

5. In the File Explorer instance that's connected to the **\\LON-SVR1\Data** folder, add the **Attributes** column in the **details** pane by right-clicking or accessing the context menu for the **Title** column in **details** pane; for example, on **Name**, select **More**, select the **Attributes** check box, and then select **OK**.
6. Drag the **Attributes** column to be next to the **Name** column, and then note the file dates and their attributes.
7. Verify the attributes of the files. Additionally, verify the size on the disk for the **Windows Server 2016 Hybrid Cloud.pdf** file by reviewing its properties.

13.5 Exercise 5: Troubleshooting replication issues

13.5.1 Task 1: Monitor File Sync replication

1. On **SEA-CL1**, use File Explorer to copy the **C:\Windows\INF** folder to **\\LON-SVR1\Data**. The folder will sync to the cloud endpoint, which will cause sync traffic.
2. In the Azure portal, browse to the **Sync1** sync group in the **FileSync1** Storage Sync Service.
3. In the **Server endpoint** section, verify that the **Health** of both endpoints has green check marks.
4. Select the `LON-SVR1.Contoso.com` endpoint in the **Server Endpoint Properties** pane, review **Sync Activity**, and then close the pane.
5. Select the **Files Synced** graph, and then explore how you can customize the graph by using a filter.
6. In File Explorer, verify if the **INF** folder is syncing to drive **Z**.
7. In the Azure portal, verify that the **INF** sync traffic is visible in the **Files Synced** and **Bytes Synced** graphs. The **INF** folder has more than 800 files, and its size is more than 40 MB.

13.5.2 Task 2: Test replication conflict resolution

1. On **SEA-CL1**, in File Explorer, verify that **File1.txt** is available in **\\LON-SVR1\Data**. Remember that you uploaded **File1.txt** to the Azure file share, from where it was synced to **SEA-SVR1** by File Sync.
2. Create a file named **Sync.txt** in **\\LON-SVR1\Data**.
3. In File Explorer, verify that the **Sync.txt** file is also on drive **Z**. Remember that drive **Z** is the mounted Azure file share, where the file was synced from **LON-SVR1** by File Sync.
4. In File Explorer, create a file named **Demo.txt** on drive **Z**.
5. In File Explorer, create a file named **Demo.txt** on **\\LON-SVR1\Data**.

   Note: You're creating files with the same name to cause a sync conflict.

6. In File Explorer, review the content of drive **Z**. Verify that drive **Z**, which is the mounted Azure file share, includes the **Demo.txt** and **Demo-LON-SVR1.txt** (or **Demo-Cloud.txt**) files. This is because File Sync detected a sync conflict and added the endpoint name (**LON-SVR1** or Cloud) to the file that caused the conflict.

   Note: You might need to wait up to a minute for the sync conflict to occur and for both files to appear on drive **Z**.

13.6 Exercise 6: Cleaning up the Azure subscription

13.6.1 Task 1: Delete the Azure resources that were created in the lab

1. On **SEA-CL1**, in the Azure portal, browse to the **FileSync1** Storage Sync Service.
2. In the **Storage Sync Service** pane, select **Registered Servers**, in the **details** pane, right-click or access the context menu for `LON-SVR1.Contoso.com`, select **Unregister server**, in the **Unregister server** pane, enter `LON-SVR1.Contoso.com` in a text box, and then select **Unregister**.
3. In **Storage Sync Service** pane, select **Registered Servers**, in the **details** pane, right-click or access the context menu for `SEA-SVR1.Contoso.com`, select **Unregister server**, in the **Unregister server** pane, enter `SEA-SVR1.Contoso.com` in a text box, and then select **Unregister**.
4. Wait until the registration for both servers is removed.
5. In the **Storage Sync Service** pane, select **Sync groups**, and then in the **details** pane, select **Sync1**.
6. In the **Sync1** pane, right-click or access the context menu for **share1** in the **cloud endpoints** section, select **Delete** and then select **OK**.
7. Wait until **share1** is deleted.
8. Select **Delete**, and then select **OK**.
9. In the **navigation** pane, select **All resources**.
10. In the **details** pane, select **FileSync1** and the Azure storage account that you created in the lab (the storage account has a name in the *<YourLowercaseInitials>DDMMYY* format).
11. In the **Delete Resources** pane, select **Delete**, enter **yes** in a text box, and then select **Delete**.
12. In the **navigation** pane, select **Resource groups**.
13. In the **details** pane select **RG1**, select **Delete resource group**, enter **RG1**, and then select **Delete**.

13.7 lab: title: 'Lab: Deploying and configuring Windows Server 2019 on Azure VMs' type: 'Answer Key' module: 'Module 6: Deploying and Configuring Azure VMs'

14 Lab answer key: Deploying and configuring Windows Server 2019 on Azure VMs

14.1 Exercise 1: Authoring Azure Resource Manager (ARM) templates for Azure VM deployment

14.1.1 Task 1: Enable the Standard tier of Security Center

In this task, you will enable the Standard tier of Azure Security Center.

Note: Skip this task and proceed directly to the next one if you have already upgraded Security Center in your Azure subscription to the Standard tier.

1. From **SEA-CL1**, start Microsoft Edge, and then navigate to the Azure portal. When prompted, sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
2. In the Azure portal, in the **Search resources, services, and docs** text box, on the toolbar, search for and select **Security Center**.
3. On the **Security Center | Getting started** blade, select **Upgrade** and then, select **Install agents**.

14.1.2 Task 2: Generate an ARM template and parameters files by using the Azure portal

In this task, you will use the Azure portal to create resource groups and create a disk in the resource group.

1. From **SEA-CL1**, start Microsoft Edge, and then navigate to the Azure portal. When prompted, sign in using a user account with the Owner or the Contributor role, in the Azure subscription you will be using in this lab.

2. In the Azure portal, in the **Search resources, services, and docs** text box, on the toolbar, search for and select **Virtual machines**. In the **Virtual machines** blade, select **+ Add** and then select **Virtual machine**.

3. In the **Create a virtual machine** blade, on the **Basics** tab, specify the following settings and leave all other settings with their default values, but do not deploy it:

   Table 1: Azure VM Basics settings

Setting	Value
Subscription	Use the name of the Azure subscription you will be using in this lab.
Resource group	ws2019-06-rg1
Virtual machine name	ws2019-06-vm0
Region	Use the name of an Azure region in which you can provision Azure virtual machi
Availability options	No infrastructure redundancy required
Image	Windows Server 2019 Datacenter-Gen1
Azure Spot instance	No
Size	Standard D2s v3
Username	Mike
Password	Pa55w.rd1234
Public inbound ports	None
Already have a Windows Server license	No

4. Select **Next: Disks >**, and then in the **Create a virtual machine** blade, on the **Disks** tab, specify the following settings, leaving all other settings with their default values:

   Table 2: Azure VM Disks settings

Setting	Value
OS disk type	Standard HDD

5. Select **Next: Networking >**, and in the **Create a virtual machine** blade, on the **Networking** tab, select *Create new** hyperlink that follows the *Virtual network** text box*.

6. On the **Create virtual network** blade, specify the following settings, leaving all other settings with their default values, and then select **OK**:

   Table 3: Azure VM virtual network settings

Setting	Value
Name	ws2019-06-vnet
Address range	10.60.0.0/20
Subnet name	subnet0
Subnet range	10.60.0.0/24

7. Back in the **Create a virtual machine** blade, on the **Networking** tab, specify the following settings, leaving all other settings with their default values:

   Table 4: Azure VM networking settings

Setting	Value
Public IP	None
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

8. Select **Next: Management >**, and in the **Create a virtual machine** blade, on the **Management** tab, specify the following settings, leaving all other settings with their default values:

Table 5: Azure VM management settings

Setting	Value
Boot diagnostics	Enabled with managed storage account (reccommended)

9. Select **Next: Advanced >**, on the **Advanced** tab of the **Create a virtual machine** blade, review the available settings without modifying any of them, and then select **Review + Create**.

   Note: Do not create the virtual machine. You will use for this purpose the autogenerated template.

14.1.3 Task 3: Download the ARM template and parameters files from the Azure portal

1. In the Azure portal, on the **Create a virtual machine** blade, select **Download a template for automation**.
2. On the **Template** blade, select **Download**.
3. Select the ellipsis button next to the **template.zip** and, in the pop-up menu, select **Show in folder**. This will automatically open File Explorer displaying the content of the **Downloads** folder.
4. In the File Explorer window, copy **template.zip** to the **C:\Labfiles\Mod06** folder on SEA-CL1 (create a new folder if needed).
5. From the **Template** blade, navigate back to the **Create a virtual machine** blade, and close it without completing the deployment.

14.2 Exercise 2: Modifying ARM templates to include VM extension-based configuration

14.2.1 Task 1: Review the ARM template and parameters files for Azure VM deployment

1. On **SEA-CL1**, start File Explorer, and then browse to the **C:\Labfiles\Mod06** folder.
2. Extract the content of the **template.zip** file into the same folder.
3. Open the **template.json** file in Notepad, and review its content. Keep the Notepad window open.
4. From File Explorer, open the **C:\Labfiles\Mod06\parameters.json** file in Notepad and review its content.
5. Close the Notepad window displaying the **parameters.json** file**.

14.2.2 Task 2: Add an Azure VM extension section to the existing template

1. On **SEA-CL1**, in the Notepad window displaying the content of the **template.json** file, insert the following code directly after the `"resources": [` line):

```
{
   "type": "Microsoft.Compute/virtualMachines/extensions",
   "name": "[concat(parameters('virtualMachineName'), '/customScriptExtension')]",
   "apiVersion": "2018-06-01",
   "location": "[resourceGroup().location]",
   "dependsOn": [
       "[concat('Microsoft.Compute/virtualMachines/', parameters('virtualMachineName'))]"
   ],
   "properties": {
       "publisher": "Microsoft.Compute",
       "type": "CustomScriptExtension",
       "typeHandlerVersion": "1.7",
       "autoUpgradeMinorVersion": true,
       "settings": {
           "commandToExecute": "powershell.exe Install-WindowsFeature -name Web-Server -Inclu
      }
   }
},
```

2. Save the change and close the file.

14.3 Exercise 3: Deploying Azure VMs running Windows Server 2019 by using ARM templates

14.3.1 Task 1: Deploy an Azure VM by using an ARM template

1. On **SEA-CL1**, switch to the browser window displaying the Azure portal.
2. In the Azure portal, on the toolbar, in the **Search resources, services, and docs** text box, search for and select **Template deployment (deploy using custom templates)**.
3. In the **Custom deployment** blade, select **Build your own template in the editor**.
4. In the **Edit template** blade, select **Load file**, upload the template file **template.json** that you edited in the previous exercise, and then select **Save**.
5. In the **Custom deployment** blade, select **Edit parameters**.
6. In the **Edit parameters** blade, select **Load file**, upload the parameters file **parameters.json** that you reviewed in the previous exercise, and then select **Save**.
7. Back in the **Custom deployment** blade, specify the following settings, and leave the other settings with their default values:

   Table 6: Custom template deployment settings

Setting	Value
Subscription	Use the name of the Azure subscription you are using in this lab.
Resource group	ws2019-06-rg1
Region	Use the name of the Azure region into which you can provision Azure VMs.
Admin Password	Pa55w.rd1234

8. Select **Review + create** and then select **Create**.
9. Verify that the deployment completed successfully.

   Note: The deployment might take about 10 minutes.

14.3.2 Task 2: Review results of the Azure VM deployment

1. In the Azure portal, on the toolbar, in the **Search resources, services, and docs** text box, search for and select **Resource groups**.
2. On the **Resource groups** blade, select the **ws2019-06-rg1** entry.
3. On the **ws2019-06-rg1** blade, on the **Overview** blade, review the list of resources, including the Azure VM **ws2019-06-vm0**.
4. Within the list of resources, select the Azure VM **ws2019-06-vm0** entry. 1. On the **ws2019-06-vm0** blade, select **Extensions**, and on the list of extensions, verify that the **customScriptExtension** has been provisioned successfully.
5. Navigate back to the **ws2019-06-rg1** blade, and in the **Settings** section, select **Deployments**.
6. On the **ws2019-06-rg1|Deployments** blade, select the **Microsoft.Template** link.
7. On the **Microsoft.Template|Overview** blade, select **Template**, and note that this is the same template you used for deployment.

14.4 Exercise 4: Configuring administrative access to Azure VMs running Windows Server 2019

14.4.1 Task 1: Verify the Azure Security Center Standard tier

1. In the Azure portal, on the toolbar, in the **Search resources, services, and docs** text box, search for and select **Security Center**.
2. On the **Security Center** blade, in the **Management** section, select **Coverage**.
3. On the **Security Center|Coverage** blade, to the right of the entry representing the Azure subscription you are using for this lab, select **Edit plan**.
4. On the **Pricing** blade, verify that the **Standard** tile is selected.

14.4.2 Task 2: Review Just in time VM access settings

1. Navigate to the **Security Center|Azure Defender** blade and under **Advanced Protection** select **Just-in-Time VM Access**.
2. On the **Security Center|Just in time VM access** blade, select the **Unsupported** tab, and note the entry representing the **ws2019-06-vm0** Azure VM.

   Note: This is expected because the Azure VM is currently not accessible from internet and doesn't have an NSG associated with its network interface. Navigate to the **Security Center|Azure Defender** blade and under **Advanced Protection** select **Just-in-Time VM Access**. **Note**: It might take about 10 minutes for the VM to appear in the Unsupported tab. You may continue with the next exercise.

14.5 Exercise 5: Configuring Windows Server 2019 security in Azure VMs

14.5.1 Task 1: Create and configure an NSG

1. In the Azure portal, on the toolbar, in the **Search resources, services, and docs** text box, search for and select **Network security groups**.
2. On the **Network security groups** blade, select **+ Add**.
3. On the **Basics** tab of the **Create network security group** blade, specify the following settings (leave others with their default values):

   Table 7: Network security group settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Name	ws2019-06-vm0-nsg1
Resource group	ws2019-06-rg1
Region	the name of the Azure region into which you provisioned the Azure VM ws2019-06-vm0

4. On the **Create network security group** blade, on the **Basics** tab of, select **Review + create**, and then select **Create**.
5. In the Azure portal, navigate back to the **ws2019-06-rg1** blade, and then in the list of resources, select the entry representing the newly created network security group **ws2019-06-vm0-nsg1**.
6. On the **ws2019-06-vm0-nsg1** blade, review the listing of the default inbound and outbound security rules, and then in the **Settings** section, select **Inbound security rules**.
7. On the **ws2019-06-vm0-nsg1|Inbound security rules** blade, select **+ Add**.
8. On the **Add inbound security rule** blade, specify the following settings, leaving all others with their default values, and then select **Add**:

   Table 8: Network security group rule settings

Setting	Value
Source	Any
Source port ranges	*
Destination	Any
Destination port ranges	80
Protocol	TCP
Action	Allow
Priority	300
Name	AllowHTTPInBound

14.5.2 Task 2: Configure Inbound HTTP access to an Azure VM

1. In the Azure portal, navigate back to the **ws2019-06-rg1** blade, and then in the list of resources, select the entry representing the Azure VM **ws2019-06-vm0**.

2. On the **ws2019-06-vm0** blade, select **Networking**.
3. On the **ws2019-06-vm0|Networking** blade, select the link designating the network interface attached to **ws2019-06-vm0**.
4. On the blade displaying the network interface properties, select **Network security group**, and then select the dropdown menu next to **None**.
5. On the **Choose network security group** blade, select **ws2019-06-vm0-nsg1**, and then select **Save**.
6. Back on the blade displaying the properties of the network interface, select **IP configurations**, and then select the **ipconfig1** entry.
7. On the **ipconfig1** blade, in the **Public IP address** section, select **Associate** and then, below the **Public IP address** drop-down list, select **Create new**.
8. In the **Add a public IP address** window, specify the following settings and then select **OK**:

   Table 9: Public IP address settings

Setting	Value
Name	ws2019-06-vm0-pip1
SKU	Standard

9. Back on the **ipconfig1** blade, select **Save**.
10. Navigate back to the blade displaying the network interface properties, select **Overview**. Note the value of the public IP address assigned to the interface.
11. Open another browser tab, navigate to that IP address, and verify that a webpage opens, displaying **Hello World from ws2019-06-vm0**.
12. From the lab computer, start the Remote Desktop app, and try connecting to the same IP address. Verify that the connection fails.

    Note: This is expected because the Azure VM is currently not accessible from internet via TCP port 3389, only via TCP port 80.

14.5.3 Task 3: Trigger re-evaluation of the JIT status of an Azure VM

Note: This task is necessary to trigger re-evaluation of the JIT status of the Azure VM. By default, this might take up to 24 hours.

1. In the Azure portal, navigate back to the **Azure Security Center** blade, and in the **Management** section, select **Coverage**.
2. On the **Security Center | Coverage** blade, select the **Edit plan** link.
3. On the **Pricing** blade, switch to the **Free** tier by selecting **Azure Defender off** and **Save**. Clear the check box **Microsoft may contact me about my feedback**, and select **Confirm**.

   Note: Wait for about 2 minutes before you proceed to the next step.
4. In the Azure portal, navigate back to the **Security Center | Getting started** blade.
5. On the **Security Center | Getting started** blade, in the **Enable standard tier on 1 subscription** blade, ensure that the check box next to your Azure subscription is selected, select the check box next to the workspace which name starts with the **DefaultWorkspace** string, select **Upgrade** and then, select **Install agents**.
6. Refresh the browser window displaying the Azure portal.

14.5.4 Task 4: Configure Inbound RDP access to the Azure VM

1. In the Azure portal, navigate back to the **Azure Security Center** blade, select **Azure Defender** in the **Cloud Security** section, and then select **Just in time VM access** in the **Advanced Protection** section.

2. On the **Security Center|Just in time VM access** blade, select the **Not configured** tab, and note the entry representing the **ws2019-06-vm0** Azure VM.
3. Select the **ws2019-06-vm0** check box, and then select **Enable JIT on 1 VMs**.
4. On the **JIT VM access configuration** blade, select and hold, right-click, or access the context menu from the ellipsis next to the **22** entry, select **Delete**, and then select **Save**.

   Note: It might take about 10 minutes for the VM to appear in the **Not configured** tab. To accelerate this process, select **Configuration** on the **ws2019-06-vm0** Azure VM and enable JIT VM access. Then select the link to **Open Azure Security Center**.

14.5.5 Task 5: Connect to the Azure VM via JIT VM access

1. Navigate back to the **ws2019-06-vm0** blade, select **Connect**, and then in the drop-down list, select **RDP**. 1. Note the message indicating that this VM has just-in-time access policy.
2. In the **Source IP** section, select **My IP**, and then select **Request access**.
3. When the request is approved, select **Download RDP File** and follow prompts to connect to the target Azure VM.
4. When prompted for credentials, specify the following values, and then select **OK**:

   Table 10: Sign-in credentials

Setting	Value
Username	Mike
Password	Pa55w.rd1234

5. Verify that you can successfully sign in to the Azure VM via Remote Desktop and close the Remote Desktop session.

14.6 Exercise 6: Deprovisioning the Azure environment

14.6.1 Task 1: Start a PowerShell session in Cloud Shell

1. Back in the Azure portal, open the **Azure Cloud Shell** blade by selecting the Cloud Shell button in the Azure portal.
2. If prompted to select either **Bash** or **PowerShell**, and then select **PowerShell**.

   Note: If this is the first time you're starting **Cloud Shell** and you're presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and then select **Create storage**.

14.6.2 Task 2: Identify all Azure resources provisioned in the lab

1. From the Cloud Shell blade, run the following command to list all resource groups created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-06-*'
   ```

2. From the Cloud Shell blade, run the following command to delete all resource groups created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-06-*'|Remove-AzResourceGroup -Force -AsJob
   ```

   Note: The command executes asynchronously (as determined by the *-AsJob* parameter), so while you will be able to run another PowerShell command immediately after within the same PowerShell session, it will take a few minutes before the resource groups are actually removed. --- lab: title: 'Lab: Managing Azure VMs running Windows Server 2019' type: 'Answer Key' module: 'Module 7: Managing and maintaining Azure VMs'

---

15 Lab answer key: Managing Azure VMs running Windows Server 2019

15.1 Exercise 1: Provisioning Azure VMs running Windows Server 2019

15.1.1 Task 1: Create a resource group

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with **Pa55w.rd** as the password.
2. On **SEA-CL1**, start Microsoft Edge, and then navigate to the Azure portal. When prompted, sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
3. In the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Resource groups**.
4. On the **Resource groups** blade, select **+ Add**.
5. On the **Create a resource group** blade, specify the following settings:

   Table 1: Resource group settings

Setting	Value
Subscription	Use the name of the Azure subscription you will be using in this lab.
Resource group	ws2019-07-rg1
Region	Use the name of an Azure region in which you can provision Azure virtual machines.

6. Select **Review + create**, wait for the validation process to complete, and then select **Create**.

15.1.2 Task 2: Upload PowerShell scripts into Cloud Shell home directory

1. On **SEA-CL1**, in the Microsoft Edge browser displaying the Azure portal, open a new browser tab and, in the address bar, enter `https://shell.azure.com`. If prompted to authenticate, sign in using a user account with the Owner role in the Azure subscription you are using in this lab.

   > **Note**: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and select **Create storage**.

2. Ensure that the **PowerShell** entry appears in the drop-down list directly under the **Azure Cloud Shell** header. If that's not the case, expand the drop down list and select **PowerShell**.
3. Select the **Upload/Download files** icon on the top menu ribbon and, in the drop-down menu, select **Upload**. This will display the **Open** dialog box.
4. In the **Open** dialog box, navigate to **C:\Labfiles\Mod07\Scripts**, and then upload the following three files:

   - **Mod07Network.ps1**
   - **Mod07GW.ps1**
   - **Mod07TG.ps1**

15.1.3 Task 3: Create two Azure VMs by using Azure Cloud Shell

1. On **SEA-CL1**, in the Microsoft Edge browser displaying the Cloud Shell, at the PowerShell prompt, enter the following command and select the **Enter** key to create virtual network resources:

   ```
   ./Mod07Network.ps1
   ```

   > **Note**: Ignore warnings regarding changes to PowerShell syntax.

2. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to create the **Mod07Gateway** VM:

   ```
   ./Mod07GW.ps1
   ```

3. When prompted, enter the following:

   Table 2: Mod07Gateway VM local Administrator credentials

Setting	Value
User	Student
Password	Pa55w.rd1234

Note: It might take about 3-5 minutes to create the **Mod07Gateway** VM.

4. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to create the **Mod07Target** VM:

   ```
   ./Mod07TG.ps1
   ```

5. When prompted, enter the following:

   Table 3: Mod07Target VM local Administrator credentials

Setting	Value
User	Student
Password	Pa55w.rd1234

Note: It might take approximately 3-5 minutes to create the **Mod07Target** VM.

Note: Leave the Azure Cloud Shell tab open - you'll use it later in this lab. After 20 minutes, the Cloud Shell will automatically disconnect, but you can select the **Reconnect** button to return to the PowerShell prompt.

15.2 Exercise 2: Managing Azure VMs running Windows Server 2019 by using Windows Admin Center

15.2.1 Task 1: Install Microsoft Edge and Windows Admin Center on the Mod07Gateway Azure VM

1. On **SEA-CL1**, in the Microsoft Edge window, switch to the tab displaying the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual machines**.
2. On the **Virtual machines** blade, select the **Mod07Gateway** entry.
3. On the **Mod07Gateway** blade, in the top menu, select **Connect**, in the drop-down menu, select **RDP**, on the **Mod07Gateway | Connect** blade, select **Download RDP File**, and, at the bottom of the browser page, select **Open**.
4. In the **Remote Desktop Connection** window, select **Connect**.
5. In the **Windows Security** window, in **User name** field, enter **Student**, in the **Password** field, enter **Pa55w.rd1234**, and then select **OK**.

   Note: If the **Windows Security**, **Enter credentials** page displays the **CONTOSO\Administrator** user name, select **More choices**, select **Use a different account**, and then enter the credentials provided in this step.

6. In the **Remote Desktop Connection** window, select **Yes**.
7. Within the Remote Desktop session to the **Mod07Gateway** Azure VM, in the Networks bar, select **No** and wait for the Server Manager window to load.
8. In **Server Manager**, in the console tree, select **Local Server**.
9. In the details pane, select the **IE Enhanced Security Configuration** item and then select the **On** hyperlink next to it.
10. In the **Internet Explorer Enhanced Security Configuration** window, under **Administrators**, select the **Off** radio button, and then select **OK**.
11. In the taskbar, select **Internet Explorer**.
12. In the **Set up Internet Explorer 11** window, select **OK**.
13. Maximize **Internet Explorer**.
14. In the address bar, enter **Microsoft Edge**, select **Enter**, and then select the **Download now** button.

15. In the **Microsoft Edge** window, select **DOWNLOAD for Windows 10**.
16. In the install window, on the **Download the new Microsoft Edge** page, select **Accept and download**.
17. Select the **Run** button in the bar displayed at the bottom of the browser page.
18. After a few moments, after Microsoft Edge installs and then opens with the **Welcome** page, select **Get started**.
19. On the **Let's set up your new tab** pane, select **Confirm**.
20. On the **See your favorites, passwords and many more on any device** pane, select **Continue without Signing-in**.

    Note: The Mod07Gateway may be need time to apply Windows Updates before the Edge browser can be installed. Installing a Chrome browser can be a quicker option.
21. In the Microsoft Edge window, navigate to Windows Admin Center
22. Select the **Windows Admin Center** link in the **Download now** section to navigate to the Windows Admin Center section of Microsoft Evaluation Center.
23. In the **Start your evaluation** section, select **Continue**, enter requested information on the download form, select **Continue**, and then select **Download**.
24. When the download completes, select the **Open file** link and, in the **Open File - Security Warning** dialog box, select **Run**. This will start the **Windows Admin Center Setup** wizard.
25. On the first page of the setup wizard, select the **I accept these terms** check box, and then select **Next**.
26. In the subsequent three pages, select **Next** each time, accepting the defaults, and on the fourth page, select **Install**.
27. When the installation completes, in the **Windows Admin Center Setup** program, select **Finish**.

15.2.2 Task 2: Add the Mod07Target VM to Windows Admin Center on Mod07Gateway VM

1. In the **Microsoft Edge** browser address bar, enter `https://Mod07Gateway`.
2. Within the Remote Desktop session to the **Mod07Gateway** Azure VM, in the Microsoft Edge window displaying **Windows Admin Center**, on the **All connections** page, select **+ Add**.
3. On the **Add or create resources** blade, in the **Servers** section, select **Add**.
4. In the **Server name** text box, enter **Mod07Target** and select **Add**.
5. On the **All connections** page, select **Mod07Target**.

15.2.3 Task 3: Use Windows Admin Center to install the Internet Information Services (IIS) Web Server role on Mod07Target

1. Within the Remote Desktop session to **Mod07Gateway**, in the Microsoft Edge browser, open a new tab and, in the address bar, enter `http://mod07target`. Note that the target page can't be reached. Keep the tab open and switch back to the **Windows Admin Center** tab.
2. In **Windows Admin Center**, on the **Mod07Target** page, in the **Tools** listing, scroll to and select **Roles & features**.
3. In the **Roles and features** details pane, scroll to and select the **Web Server (IIS)** check box and then, in the top area of the details pane, select **+ Install**.
4. On the **Install Roles and Features** pane, in the **Continue installation?** section, select **Yes**.
5. In the **Tools** listing, select **Overview** and then, in the toolbar of the Overview pane, select **Refresh**. You can watch the CPU activity corresponding to the installation of the Web Server role.

   Note: Completion of the installation will display a notification. You can review it by selecting the **Notifications** icon in the upper right corner of the page.
6. Once the installation completes, switch to the Microsoft Edge tab targeting the `http://mod07target` URL and refresh the browser page. Verify that the browser displays the **Internet Information Services Welcome** page.
7. Switch back to browser tab displaying **Windows AdminCenter**, in the details pane top toolbar, select **Shutdown**, and then in the **Shut down the computer** window, select **Yes**.

8. Leave the Remote Desktop connection to **Mod07Gateway** open.

15.3 Exercise 3: Managing Windows Server 2019 running in Azure VMs by using PowerShell Remoting

15.3.1 Task 1: Configure PowerShell Remoting of an Azure VM running Windows Server 2019

1. On **SEA-CL1**, in the Microsoft Edge window, switch to the tab displaying Azure Cloud Shell. If needed, select **Reconnect**.
2. From the Cloud Shell blade, run the following commands to disable certificate verification for PowerShell remoting.

   ```
   install-module pswsman
   Disable-WSManCertVerification -All
   ```

3. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to start the **Mod07Target** Azure VM:

   ```
   Start-AzVM -ResourceGroupName ws2019-07-rg1 -Name Mod07Target
   ```

4. After the VM successfully starts, in the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to configure PowerShell Remoting on the **Mod07Target** Azure VM:

   ```
   Enable-AzVMPSRemoting -Name 'Mod07Target' -ResourceGroupName 'ws2019-07-rg1' -Protocol https -OsTy
   ```

   Note: The **Enable-AzureVMPSRemoting** cmdlet configures WinRM on the target VM and configures its Network Security Group to allow access via Windows Remote Management.

15.3.2 Task 2: Manage Windows Server 2019 running in an Azure VM by using PowerShell Remoting

1. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to list Windows services which names begin with **Win** installed within the operating system of the **Mod07Target** Azure VM:

   ```
   Invoke-AzVMCommand -Name 'Mod07Target' -ResourceGroupName 'ws2019-07-rg1' -ScriptBlock {get-servic
   ```

2. At the **User:** prompt, enter **Student**, and then select the **Enter** key.
3. At the **Password for user Student:** prompt, enter **Pa55w.rd1234**, and then select the **Enter** key.
4. Review the results displayed in the Cloud Shell pane and verify that they include a list of services which names begin with **Win**.
5. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to start an interactive PowerShell Remoting session within the operating system of the **Mod07Target** Azure VM:

   ```
   Enter-AzVM -Name Mod07Target -ResourceGroupName ws2019-07-rg1 -Credential $Cred
   ```

6. At the **User:** prompt, enter **Student**, and then select the **Enter** key.
7. At the **Password for user Student:** prompt, enter **Pa55w.rd1234**, and then select the **Enter** key.

   Note: You will be presented with an interactive session prompt. This allows you to run Windows PowerShell cmdlets directly against the target VM until you exit the session.

8. At the PowerShell Remoting session, enter the following command and select the **Enter** key to list locally installed Windows services which names begin with **Win**:

   ```
   Get-Service Win*
   ```

   Note: The results should include the same list of services that you reviewed earlier in this task.

9. At the PowerShell Remoting session, enter the following command and select the **Enter** key to exit the interactive PowerShell Remoting session.

   ```
   Exit
   ```

Note: Keep the **Cloud Shell** tab open. You will use it again later in this lab.

15.4 Exercise 4: Managing Windows Server 2019 running in Azure VMs by using Run command

15.4.1 Task 1: Use EnableRemotePS command

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual machines**.
2. On the **Virtual machines** blade, select the **Mod07Target** entry.
3. On the **Mod07Target** blade, in the console tree, scroll down to the **Operations** section and select the **Run command** item.
4. On the **Mod07Target | Run command** blade, select the **EnableRemotePS** item.
5. On the **Run Command Script** blade, select **Script**, review the content of the script that enables PowerShell Remoting on the target operating system, and select **Run**.
6. Wait until script execution completes.

15.4.2 Task 2: Use RunPowerShellScript command

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual machines**.
2. On the **Virtual machines** blade, select the **Mod07Target** entry.
3. On the **Mod07Target** blade, in the console tree, scroll down to the **Operations** section and select the **Run command** item.
4. On the **Mod07Target | Run command** blade, select the **RunPowerShellScript** item.
5. On the **Run Command Script** blade, in the **PowerShell Script** pane, enter `Get-Service Win*` and select **Run**.
6. Wait until script execution completes, examine the results, and verify that they include the same list of services that you reviewed in the previous task.
7. Close the **Run Command Script** blade.

15.5 Exercise 5: Managing Windows Server 2019 in Azure VMs by using the serial console

15.5.1 Task 1: Create a storage account

Note: Storage account names must be globally unique and can contain between 3 and 24 characters, including lowercase letters and numbers, starting with a letter.

1. On **SEA-CL1**, in the Microsoft Edge browser, in the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Storage accounts**.
2. On the **Storage accounts** blade, select **+ Add**.
3. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others with their default values):

Table 4: Storage account settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-07-rg1
Storage account name	any globally unique name between 3 and 24 in length consisting of letters and digits
Location	the name of the Azure region where you created the resource group in the previous task
Performance	Standard
Account kind	Storage (general purpose v1)
Replication	Locally redundant storage (LRS)

4. On the **Basics** tab of the **Create storage account** blade, select **Review + Create**, wait for the validation process to complete, and select **Create**.

Note: Wait for the Storage account to be created. This should take about 2 minutes.

15.5.2 Task 2: Configure boot diagnostics for an Azure VM

1. On **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual machines**.
2. On the **Virtual machines** blade, select **Mod07Target**.
3. In the console tree, scroll down to the **Support + troubleshooting** section and select **Boot diagnostics**.
4. On the **Mod07Target | Boot diagnostics** blade, in the top menu bar, select **Settings**.
5. On the **Boot diagnostics** blade, select the **Enable with custom storage account** option, in the **Diagnostics storage account** section, select the storage account you created earlier in this exercise, and select **Save**.

   Note: Managed storage account does not support the serial console functionality.

15.5.3 Task 3: Use the serial console

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, on the **Mod07Target** blade, in the console tree, scroll down to the **Support + troubleshooting** section and select **Serial console**.

   Note: The **Mod07Target | Serial console** blade should display the **SAC> ** prompt
2. On **Mod07Target | Serial console** blade, at the **SAC> ** prompt, enter **cmd** and select the **Enter** key to create a channel that contains a CMD instance.
3. On **Mod07Target | Serial console** blade, at the **SAC> ** prompt, enter **ch -si 1** and select the **Enter** key to switch to the channel that's running the CMD instance.
4. On **Mod07Target | Serial console** blade, select the **Enter** key, and then enter the following sign-in credentials of the local Administrator account:

   Table 5: Mod07Target VM local Administrator credentials

Setting	Value
User	Student
Domain	Mod07Target
Password	Pa55w.rd1234

5. On **Mod07Target | Serial console** blade, at the **C:\windows\system32** prompt, enter the following commands, selecting the Enter key after each command in order to configure operating system boot options:

   ```
   bcdedit /set {bootmgr} displaybootmenu yes
   bcdedit /set {bootmgr} timeout 20
   bcdedit /set {bootmgr} bootems yes
   shutdown -r -t 0
   ```
6. On **Mod07Target | Serial console** blade, when the EMS window displays, select the **F8** key to display the **Advanced Boot Option** screen.
7. On **Mod07Target | Serial console** blade, within the serial console session, use the arrows on the keyboard to navigate the **Advanced Boot Option** screen and select the **Start Windows normally** option.
8. On **Mod07Target | Serial console** blade, exit the serial console by selecting the **Overview** node in the console tree.

   Note: The **Advanced Boot options** screen displays the message, **Choose Advanced Options for: Windows server 2016**. Mod07Target is running Windows Server 2019. This is expected, since the serial console code has not been updated on Windows Server 2019.

15.6 Exercise 6: Managing Windows Server 2019 in Azure VMs by using Azure Policy Guest Configuration

15.6.1 Task 1: Enable the Guest Configuration resource provider.

1. On **SEA-CL1**, in the Microsoft Edge window, switch to the tab displaying Azure Cloud Shell. If needed, select **Reconnect**.
2. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to register the Guest Configuration resource provider:

   ```
   Register-AzResourceProvider -ProviderNamespace 'Microsoft.GuestConfiguration'
   ```

3. Wait until the resource provider is registered.

   > **Note**: To verify the registration status, you can re-run the **Register-AzResourceProvider** cmdlet.

15.6.2 Task 2: Assign an Azure Policy Guest Configuration by using the Azure portal

1. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, search for and select **Policy**.
2. On the **Policy** blade, in the **Authoring** section, select **Definitions**.
3. On the **Policy | Definitions** blade, in the filter bar above the details pane, in the **Category** column, select the **All categories** drop-down list.
4. In the list, clear the check box **Select all**, and then select **Guest Configuration** only.
5. In the filter bar above the details pane, in the **Definition type** column, select the **All Definitions** drop-down list, and then select **Initiative**.
6. In the details pane, select **Audit Windows VMs on which the specified services are not installed and 'Running'** item.

   > **Note**: Alternatively, you can enter **Audit Windows VMs on which the specified services are not installed and 'Running'** in the **Search** text box.

7. On the **Audit Windows VMs on which the specified services are not installed and 'Running'** blade, select **Assign**.
8. On the **Basics** tab of the **Audit Windows VMs on which the specified services are not installed and 'Running'** blade, select the ellipses icon next to the **Scope** text box.
9. On the **Scope** blade, in the **Subscription** drop-down list, select your subscription, in the **Resource group** drop-down list, select **ws2019-07-rg1**, and then select **Select**.
10. Back on the **Basics** tab of the **Audit Windows VMs on which the specified services are not installed and 'Running'** blade, in the **Description** text box, enter **Auditing Windows services settings** and then select **Next**.
11. In the **Parameters** tab of the **Audit Windows VMs on which the specified services are not installed and 'Running'** blade, in the **Service names (supports wildcards)** text box, enter **W3SVC** and select **Next**.

    > **Note**: **W3SVC** is the name of the World Wide Web Publishing Service, which you installed on **Mod07Target** earlier in this lab.

12. On the **Remediations** tab of the **Audit Windows VMs on which the specified services are not installed and 'Running'** blade, select the **Create a remediation task** checkbox, leave the default entry in the **Policy to remediate** drop-down list, in the **Managed identity location** drop-down list, select the Azure region into which you deploye all resources in this lab, and select **Next**.
13. On the **Review + create** tab of the **Audit Windows VMs on which the specified services are not installed and 'Running'** blade, select **Create**.

15.6.3 Task 3: Review results of the Guest Configuration policy.

1. On **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, navigate back to the **Policy | Definitions** blade and, in the console tree, select **Overview**.

2. On the **Policy** blade, note the **Audit Windows VMs on which the specified services are not installed and 'Running'** entry and verify that its **Compliance state** is listed as **Not started**
3. On **SEA-CL1**, in the Microsoft Edge window, switch to the tab displaying Azure Cloud Shell. If needed, select **Reconnect**.
4. In the Cloud Shell window, at the PowerShell prompt, enter the following command and select the **Enter** key to trigger an on-demand Azure Policy compliance scan targeting resources in the resource group **ws2019-07-rg1**:

   ```
   Start-AzPolicyComplianceScan -ResourceGroupName 'ws2019-07-rg1'
   ```

   > **Note**: Wait for the compliance scan to complete. For information regarding time it takes to complete different types of Azure Policy processing, refer to Evaluation triggers and Validation frequency.
   >
   > **Note**: Since you installed Web Server (IIS) server role on **Mod07Target**, that VM should be listed as compliant. However, since the resource group **ws2019-07-rg1** also contains the **Mod07Gateway** VM which does not include the Web Server (IIS) server role, the state of that resource and the assignment should be listed as **Non-compliant**.

5. To verify compliance status of individual resources, on **SEA-CL1**, in the Microsoft Edge window displaying the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Virtual machines**.
6. On the **Virtual machines** blade, select the **Mod07Target** entry.
7. On the **Mod07Target** blade, in the console tree, scroll to the **Operations** section, and then select **Policies**.
8. Verify that the **Audit Windows VMs on which the specified services are not installed and 'Running'** policy is listed as **Compliant**.
9. Navigate back to the **Virtual machines** blade and select the **Mod07Gateway** entry.
10. On the **Mod07Gateway** blade, in the console tree, scroll to the **Operations** section, and then select **Policies**.
11. Verify that the **Audit Windows VMs on which the specified services are not installed and 'Running'** policy is listed as **Non-compliant**.

15.7 Exercise 7: Deprovisioning the Azure lab environment

15.7.1 Task 1: Remove the policy assignment

1. On SEA-CL1, in the Microsoft Edge window displaying the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, search for and select **Policy**.
2. On the **Policy** blade, in the **Authoring** section, select **Assignments**.
3. On the **Policy | Assignments** blade, right-click or access the context menu for the **Audit Windows VMs on which the specified services are not installed and 'Running'** assignment and, in the context menu, select **Delete assignment**.
4. When prompted for confirmation, select **Yes**.

15.7.2 Task 2: Delete the ws2019-07-rg1 resource group

1. In the Azure portal, in the **Search resources, services, and docs** text box in the toolbar, search for and select **Resource groups**.
2. On the **Resource groups** blade, select **ws2019-07-rg1**.
3. On the **ws2019-07-rg1** blade, in the toolbar, select **Delete resource group**.
4. When prompted for confirmation, on the **Are you sure you want to delete "ws2019-07-rg1"?** blade, in the **TYPE THE RESOURCE GROUP NAME:** text box, enter **ws2019-07-rg1**, and then select **Delete**.

15.8 lab: title: 'Lab: Implementing Azure-based recovery services' type: 'Answer Key' module: 'Module 8: Planning and implementing migration and recovery services in hybrid scenarios'

16 Lab answer key: Implementing Azure-based recovery services

16.1 Exercise 1: Implementing the lab environment

16.1.0.1 Task 1: Deploy an Azure VM running Windows Server 2019 with the Hyper-V role installed

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with **Pa55w.rd** as the password.
2. On **SEA-CL1**, start Microsoft Edge, and then navigate to the Azure portal. When prompted, sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
3. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Resource groups**.
4. On the **Resource groups** blade, select **+ Add**.
5. On the **Create a resource group** blade, specify the following settings:

   Table 1: Resource group settings

Setting	Value
Subscription	Use the name of the Azure subscription you will be using in this lab.
Resource group	ws2019-08-rg1
Region	Use the name of an Azure region in which you can provision Azure virtual machines.

6. Select **Review + create**, wait for the validation process to complete, and then select **Create**.
7. On **SEA-CL1**, open another Microsoft Edge tab, navigate to 301-nested-vms-in-virtual-network Azure QuickStart template, and then select **Deploy to Azure**. This will automatically redirect the browser to the **Hyper-V Host Virtual Machine with nested VMs** blade in the Azure portal.
8. On the **Hyper-V Host Virtual Machine with nested VMs** blade in the Azure portal, specify the following settings (leave the others with their default values):

   Table 2: QuickStart template deployment settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-08-rg1
Host Public IP Address Name	ws2019-08-hvm0-pip
Virtual Network Name	ws2019-08-hv-vnet
Host Network Interface1Name	ws2019-08-hvm0-nic1
Host Network Interface2Name	ws2019-08-hvm0-nic2
Host Virtual Machine Name	ws2019-08-hvm0
Host Admin Username	Student
Host Admin Password	Pa55w.rd1234

9. On the **Hyper-V Host Virtual Machine with nested VMs** blade, select **Review + create** and then select **Create**.

   Note: Wait for the deployment to complete. The deployment might take about 10 minutes.

16.1.0.2 Task 2: Connect to the Azure VM running the Windows Server 2019 with the Hyper-V role installed

1. On **SEA-CL1**, on the Microsoft Edge tab displaying the Azure Portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Virtual machines**.
2. In the Azure portal, on the **Virtual machines** blade, select **ws2019-08-hvm0**.

3. On the **ws2019-08-hvm0** blade, select **Networking**.
4. On the **ws2019-08-hvm0 | Networking** blade, select **ws2019-08-hvm0-nic1** and then select **Add inbound port rule**.

   Note: Make sure that you modify the settings of **ws2019-08-hvm0-nic1**, which has the public IP address assigned to it.

5. On the **Add inbound security rule** blade, specify the following settings (leave the others with their default values), and then select **Add**:

   Table 3: Inbound security rule settings

Setting	Value
Destination port ranges	3389
Protocol	Any
Name	AllowRDPInBound

6. On the **ws2019-08-hvm0 | Networking** blade, select **Overview**.
7. On the **ws2019-08-hvm0** blade, in the top menu, select **Connect**, in the drop-down menu, select **RDP**, on the **ws2019-08-hvm0 | Connect** blade, select **Download RDP File**, and, at the bottom of the browser page, select **Open**.
8. In the **Remote Desktop Connection** window, select **Connect**.
9. In the **Windows Security** window, in **User name** field, enter **Student**, in the **Password** field, enter **Pa55w.rd1234**, and then select **OK**.

   Note: If the **Windows Security**, **Enter credentials** page displays the **CONTOSO\Administrator** user name, select **More choices**, select **Use a different account**, and then enter the credentials provided in this step.

10. In the **Remote Desktop Connection** window, select **Yes**.
11. Within the Remote Desktop session to the **ws2019-08-hvm0** Azure VM, in the Networks bar, select **No** and wait for the Server Manager window to load.

16.1.0.3 Task 3: Download a Windows Server 2019 VHD file

1. Within the Remote Desktop session to the **ws2019-08-hvm0** Azure VM, in **Server Manager**, in the console tree, select **Local Server**.
2. In the details pane, select the **IE Enhanced Security Configuration** item and then select the **On** hyperlink next to it.
3. In the **Internet Explorer Enhanced Security Configuration** window, under **Administrators**, select the **Off** option, and then select **OK**.
4. In the taskbar, select **Internet Explorer**.
5. In the **Set up Internet Explorer 11** window, select **OK**.
6. In Internet Explorer, browse to the Windows Server Evaluations Microsoft website and scroll down to the **Windows Server 2019** section.
7. In the **Start your evaluation** subsection of the **Windows Server 2019** section, select the **VHD** option, select **Continue**, enter requested information on the download form, select **Continue**, and then select **Download**.
8. When prompted, in the browser window, at the bottom of the page, select **Save** and wait for the download to complete.
9. When the download completes, in the browser window, at the bottom of the page, select **Open folder**.
10. In the **File Explorer** window, right-click or access the context menu for the newly downloaded VHD file, and then select **Cut**. In the navigation pane, right-click or access the context menu for **Hyper-V (F:)**, select **New**, and then select **Folder**. In the details pane, select **New folder** and select its name again, enter **VHDs** to rename it, and select the Enter key twice to open it.

11. Right-click or access the context menu for the empty area in the details pane and then select **Paste** to paste the VHD file you copied in the previous step.

16.1.0.4 Task 4: Deploy a Windows Server 2019 Hyper-V VM within an Azure VM

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Server Manager window, select **Tools** and, in the drop-down menu, select **Hyper-V Manager**.
2. In the **Hyper-V Manager** console, select the **ws2019-08-hvm0** node, select **New** and, in the cascading menu, select **Virtual Machine**. This will start the **New Virtual Machine Wizard**.
3. On the **Before You Begin** page of the **New Virtual Machine Wizard**, select **Next >**.
4. On the **Specify Name and Location** page of the **New Virtual Machine Wizard**, specify the following settings, and then select **Next >**:

   Table 4: New virtual machine name and location settings

Setting	Value
Name	ws2019-08-vm1
Store the virtual machine in a different location	selected
Location	F:\VMs

5. On the **Specify Generation** page of the **New Virtual Machine Wizard**, ensure that the **Generation 1** option is selected, and then select **Next >**:
6. On the **Assign Memory** page of the **New Virtual Machine Wizard**, set **Startup memory** to **2048**, select the **Use Dynamic Memory for this virtual machine** checkbox, and select **Next >**.
7. On the **Configure Networking** page of the **New Virtual Machine Wizard**, in the **Connection** drop-down list, select **NestedSwitch**, and then select **Next >**.
8. On the **Connect Virtual Hard Disk** page of the **New Virtual Machine Wizard**, select the option **Use an existing virtual hard disk**, select **Browse**. In the **Open** window, browse to the **F:\VHDs** folder, select the VHD file you downloaded in the previous task, and select **Open**.
9. Back on the **Connect Virtual Hard Disk** page, select **Next >**.
10. On the **Summary** page of the **New Virtual Machine Wizard**, select **Finish**.
11. In the **Hyper-V Manager** console, select the newly created virtual machine and, in the **Actions** pane, select **Start**.
12. In the **Hyper-V Manager** console, verify that the virtual machine is running and, in the **Actions** pane, select **Connect**.
13. In the Virtual Machine Connection window to **ws2019-08-vm1**, on the **Hi there** page, select **Next**.
14. In the Virtual Machine Connection window to **ws2019-08-vm1**, on the **License terms** page, select **Accept**.
15. In the Virtual Machine Connection window to **ws2019-08-vm1**, on the **Customize settings** page, set the password of the built-in Administrator account to **Pa55w.rd1234** and select **Finish**.
16. In the Virtual Machine Connection window to **ws2019-08-vm1**, select the **Action** menu and, in the drop-down menu, select **Ctrl+Alt+Delete**.
17. In the **Password** text box, enter **Pa55w.rd1234** and select the **Enter** key.
18. In the Virtual Machine Connection window to **ws2019-08-vm1**, right-click or access the context menu for the **Start** menu icon, and then select **Windows PowerShell (Admin)**.
19. From the **Administrator: Windows PowerShell** window, run the following to set the computer name:

    ```
    Rename-Computer -NewName 'ws2019-08-vm1' -Restart
    ```

    Note: The command will rename the operating system and restart it.

16.2 Exercise 2: Creating and configuring an Azure Site Recovery vault

16.2.0.1 Task 1: Create an Azure Site Recovery vault

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Internet Explorer window, navigate to the Azure portal, and sign in by providing credentials of a user account with the Owner role in the subscription you are using in this lab.
2. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, select **+ Add**.
3. On the **Basics** tab of the **Create Recovery Services vault** blade, specify the following settings (leave others with their default values) and select **Review + create**:

   Table 5: Recovery Services vault settings

Setting	Value
Subscription	The name of the Azure subscription you are using in this lab
Resource group	Select Create new, in the Name text box, enter ws2019-08-rg2 and select OK
Vault name	ws2019-08a-rsvault
Location	The name of an Azure region different from the one into which you deployed the Azure VM in the first e

4. On the **Review + create** tab of the **Create Recovery Services vault** blade, select **Create**:

   Note: By default, the default configuration for Storage Replication type is set to Geo-redundant (GRS) and Soft Delete is enabled. You will change these settings in the lab to simplify deprovisioning, but you should use them in your production environments.

16.2.0.2 Task 2: Configure the Azure Site Recovery vault

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, select **ws2019-08a-rsvault**.
2. On the **ws2019-08a-rsvault** blade, in the vertical menu, in the **Settings** section, select **Properties**.
3. On the **ws2019-08a-rsvault | Properties** blade, select the **Update** link under the **Backup Configuration** label.
4. On the **Backup Configuration** blade, set **Storage replication type** to **Locally-redundant**, select **Save** and close the **Backup Configuration** blade.

   Note: Storage replication type cannot be changed once you implement protection.
5. On the **ws2019-08a-rsvault | Properties** blade, select the **Update** link under the **Security Settings** label.
6. On the **Security Settings** blade, set **Soft Delete** to **Disable**, select **Save** and close the **Security Settings** blade.

16.3 Exercise 3: Implementing Hyper-V VM protection by using Azure Site Recovery vault

16.3.0.1 Task 1: Implement an Azure recovery site

1. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Virtual networks** and, on the **Virtual networks** blade, select **+ Add**.
2. On the **Basics** tab of the **Create virtual network** blade, specify the following settings (leave others with their default values) and select **Next: IP Addresses**:

   *Table 6: Virtual network **ws2019-08-dr-vnet** settings*

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	select Create new, in the Name text box, enter ws2019-08-rg3 and select OK

Setting	Value
Name	ws2019-08-dr-vnet
Region	the name of the Azure region into which you deployed the Recovery Services vault earlier in this lab

3. On the **IP addresses** tab of the **Create virtual network** blade, select the recycle bin icon, in the **IPv4 address space** text box, enter **10.8.0.0/22** and select **+ Add subnet**.
4. On the **Add subnet** blade, specify the following settings (leave others with their default values) and select **Add**:

   *Table 7: Virtual network **ws2019-08-dr-vnet** subnet **subnet0** settings*

Setting	Value
Subnet name	subnet0
Subnet address range	10.8.0.0/24

5. Back on the **IP addresses** tab of the **Create virtual network** blade, select **Review + create**.
6. On the **Review + create** tab of the **Create virtual network** blade, select **Create**.
7. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Virtual networks** and, on the **Virtual networks** blade, select **+ Add**.
8. On the **Basics** tab of the **Create virtual network** blade, specify the following settings (leave others with their default values) and select **Next: IP Addresses**:

   *Table 8: Virtual network **ws2019-08-test-vnet** settings*

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-08-rg3
Name	ws2019-08-test-vnet
Region	the name of the Azure region into which you deployed the Recovery Services vault earlier in this lab

9. On the **IP addresses** tab of the **Create virtual network** blade, select the recycle bin icon, in the **IPv4 address space** text box, enter **10.0.0.0/22** and select **+ Add subnet**.
10. On the **Add subnet** blade, specify the following settings (leave others with their default values) and select **Add**:

    *Table 9: Virtual network **ws2019-08-test-vnet** subnet **subnet3** settings*

Setting	Value
Subnet name	subnet3
Subnet address range	10.0.2.0/24

    Note: This matches the IP address range of the production network and the subnet containing the Hyper-V that needs to be protected.

11. Back on the **IP addresses** tab of the **Create virtual network** blade, select **Review + create**.
12. On the **Review + create** tab of the **Create virtual network** blade, select **Create**.
13. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Storage accounts** and, on the **Storage accounts** blade, select **+ Add**.
14. On the **Basics** tab of the **Create storage account** blade, specify the following settings (leave others with their default values):

    Table 10: Storage account settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	ws2019-08-rg3
Storage account name	any globally unique name between 3 and 24 in length consisting of letters and digits, starting with
Location	the name of the Azure region into which you deployed the Recovery Services vault earlier in this la
Performance	Standard
Account kind	Storage (general purpose v1)
Replication	Locally redundant storage (LRS)

15. On the **Basics** tab of the **Create storage account** blade, select **Review + create**.
16. On the **Review + create** tab of the **Create storage account** blade, select **Create**.

16.3.0.2 Task 2: Prepare protection of a Hyper-V virtual machine

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, select the **ws2019-08a-rsvault** entry.
2. On the **ws2019-08a-rsvault** blade, in the vertical menu, in the **Getting started** section, select **Site Recovery**
3. On the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure**.
4. On the **Deployment planning** tab of the **Prepare infrastructure** blade, in the **Deployment planning completed?** drop-down list, select **Yes, I have done it** and select **Next**.
5. On the **Source settings** tab of the **Prepare infrastructure** blade, next to the **Are you Using System Center VMM to manage Hyper-V hosts** label, select the **No** option.
6. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V site** link, on the **Create Hyper-V Site** blade, in the **Name** text box, enter **ws2019-08 Hyper-V site** and select **OK**:
7. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V server** link.
8. On the **Add Server** blade, select the **Download** link in step 3 of the procedure for adding on-premises Hyper-V hosts in order to download the Microsoft Azure Site Recovery Provider.
9. When prompted, in the browser window, select **Run** to launch **AzureSiteRecoveryProvider.exe**. This will start the **Azure Site Recovery Provider Setup (Hyper-V server)** wizard.
10. On the **Microsoft Update** page, select **Off** and select **Next**.
11. On the **Provider installation** page, select **Install**.
12. Switch to the Azure portal and, on the **Add Server** blade, select the **Download** button in step 4 of the procedure for registering on-premises Hyper-V hosts in order to download the vault registration key. When prompted, select **Save** to save the vault credentials file in the **Downloads** folder.
13. Switch to the **Provider installation** wizard window and select **Register**. This will start the **Microsoft Azure Site Recovery Registration Wizard**.
14. On the **Vault Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Browse**, in the **Open** window, navigate to the **Downloads** folder, select the vault credentials file, and select **Open**.
15. Back on the **Vault Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Next**.
16. On the **Proxy Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, accept the default settings and select **Next**.
17. On the **Registration** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Finish**.

18. Switch back to the Internet Explorer window displaying the Azure portal and refresh the page. When prompted, select **Leave this page**.
19. Back on the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure**.
20. On the **Deployment planning** tab of the **Prepare infrastructure** blade, in the **Deployment planning completed?** drop-down list, select **Yes, I have done it** and select **Next**.
21. On the **Source settings** tab of the **Prepare infrastructure** blade, next to the **Are you Using System Center VMM to manage Hyper-V hosts** label, select the **No** option.
22. Verify that the **Hyper-V site** and **Hyper-V servers** settings are set correctly and select **Next**.
23. On the **Target settings** tab of the **Prepare infrastructure** blade, accept the default settings and select **Next**.
24. On the **Replication policy** tab of the **Prepare infrastructure** blade, select **Create new policy and associate**.
25. On the **Create and associate policy** blade, specify the following settings (leave others with their default values) and select **OK**:

    Table 11: Policy settings

Setting	Value
Name	ws2019-08 replication policy
Copy frequency	30 seconds

26. Back on the **Replication policy** tab of the **Prepare infrastructure** blade, wait until the site has been associated with the policy and select **Next**.
27. On the **Review** tab of the **Prepare infrastructure** blade, select **Prepare**.

16.3.0.3 Task 3: Enable replication of a Hyper-V virtual machine

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Azure portal, on the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **2. Enable replication**.
2. On the **Source environment** tab of the **Enable replication** blade, in the **Source location** drop-down list, select **ws2019-08 Hyper-V site** and select **Next**.
3. On the **Target environment** tab of the **Enable replication** blade, specify the following settings (leave others with their default values) and select **Next**:

    Table 12: Target environment settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Post-failover resource group	ws2019-08-rg3
Post-failover deployment model	Resource Manager
Storage account	the name of the storage account you created in the first task of this exercise
Azure network	Configure now for selected machines
Virtual network	ws2019-08-dr-vnet
Subnet	subnet0 (10.8.0.0/24)

4. On the **Virtual machine selection** tab of the **Enable replication** blade, select the **ws2019-08-vm1** checkbox and select **Next**.
5. On the **Replication settings** tab of the **Enable replication** blade, in the **Defaults** row and **OS type** column, select **Windows** from the drop-down list and select **Next**.
6. On the **Replication policy** tab of the **Enable replication** blade, accept the default settings and select **Next**.

7. On the **Review** tab of the **Enable replication** blade, select **Enable replication**.

16.3.0.4 Task 4: Review Azure VM replication settings

1. In the Azure portal, back on the **ws2019-08a-rsvault | Site Recovery** blade, in the vertical menu, select **Replicated items**.
2. On the **ws2019-08a-rsvault | Replicated items** blade, ensure that there is an entry representing the **ws2019-08-vm1** virtual machine and verify that its **Replication Health** is listed as **Healthy** and that its **Status** is listed as either **Enabling protection** or displaying a current percentage of synchronization progress.

   Note: You might need to wait a few minutes until the **ws2019-08-vm1** entry appears on the **ws2019-08a-rsvault | Replicated items** blade.
3. On the **ws2019-08a-rsvault | Replicated items** blade, select the **ws2019-08-vm1** entry.
4. On the **ws2019-08-vm1** replicated items blade, review the **Health and status**, **Failover readiness**, **Latest recovery points**, and **Infrastructure view** sections. Note the **Planned Failover**, **Failover** and **Test Failover** toolbar icons.

   Note: Wait until the status changes to **Protected**. This might take additional 15 minutes. You will need to refresh the browser page for the status to be updated. While waiting for the replication of the nested VM to complete, proceed to Exercise 4.
5. On the **ws2019-08-vm1** replicated items blade, select **Latest recovery points** and review **Latest crash-consistent** and **Latest app-consistent** recovery points.

16.3.0.5 Task 5: Perform a failover of the Hyper-V virtual machine

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the browser window displaying the Azure portal, on the **ws2019-08-vm1** replicated items blade, select **Test failover**.
2. On the **Test failover** blade, specify the following settings (leave others with their default values) and select **OK**:

   Table 13: Test failover settings

Setting	Value
Choose a recovery point	the default option
Azure virtual network	ws2019-08-test-vnet

3. In the Azure portal, navigate back to the **ws2019-08a-rsvault** blade and, in the vertical menu, in the **Monitoring** section, select **Site Recovery jobs**. Wait until the status of the **Test failover** job is listed as **Successful**.
4. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Virtual machines** and, on the **Virtual machines** blade, note the entry representing the newly provisioned virtual machine **ws2019-08-vm1-test**.
5. In the Azure portal, navigate back to the **ws2019-08-vm1** replicated item blade and select **Cleanup test failover**.
6. On the **Test failover cleanup** blade, select the checkbox **Testing is complete. Delete test failover virtual machine(s)** and select **OK**.
7. Once the test failover cleanup job completes, refresh the browser page displaying the **ws2019-08-vm1** replicated items blade and note that you have the option to perform planned and unplanned failover.
8. On the **ws2019-08-vm1** replicated items blade, select **Planned failover**.
9. On the **Planned failover** blade, note that the failover direction settings are already set and not modifiable.
10. Close the **Planned failover** blade without initiating a failover and, on the **ws2019-08-vm1** replicated items blade, select **Failover**.
11. On the **Failover** blade, note that you have the option to choose a recovery point.

12. Close the **Failover** blade without initiating a failover.

16.4 Exercise 4: Implementing Azure Backup

16.4.0.1 Task 1: Create an Azure Site Recovery vault

Note: While, in general, the same vault can be used to implement Azure Site Recovery and Azure Backup functionality, the one hosting Azure Backup should be located close to the location of the backed up items. For this reason, you will create another Azure Site Recovery vault in the same Azure region as the Azure VM you deployed in the second exercise of this lab.

1. Within the Remote Desktop session to **ws2019-08-hvm0**, switch to the Virtual Machine Connection window to **ws2019-08-vm1**.
2. In the Virtual Machine Connection window to **ws2019-08-vm1**, in **Server Manager**, in the console tree, select **Local Server**.
3. In the details pane, select the **IE Enhanced Security Configuration** item and then select the **On** hyperlink next to it.
4. In the **Internet Explorer Enhanced Security Configuration** window, under **Administrators**, select the **Off** option, and then select **OK**.
5. In the taskbar, select **Internet Explorer**.
6. In the **Set up Internet Explorer 11** window, select **OK**.
7. In Internet Explorer, navigate to the Azure portal. When prompted, sign in using a user account with the Owner role in the Azure subscription you will be using in this lab.
8. In the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, select **+ Add**.
9. On the **Basics** tab of the **Create Recovery Services vault** blade, specify the following settings (leave others with their default values) and select **Review + create**:

   Table 14: Recovery Services vault (for Azure Backup) settings

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	select Create new, in the Name text box, enter ws2019-08-rg4 and select OK
Vault name	ws2019-08b-rsvault
Location	the name of an Azure region into which you deployed the Azure VM in the first exercise of this lab

10. On the **Review + create** tab of the **Create Recovery Services vault** blade, select **Create**:

    Note: By default, the default configuration for Storage Replication type is set to Geo-redundant (GRS) and Soft Delete is enabled. You will change these settings in the lab to simplify deprovisioning, but you should use them in your production environments.

16.4.0.2 Task 2: Configure the Azure Site Recovery vault

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the Internet Explorer window displaying the Azure portal, use the **Search resources, services, and docs** text box in the toolbar to search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, select **ws2019-08b-rsvault**.
2. On the **ws2019-08b-rsvault** blade, in the vertical menu, in the **Settings** section, select **Properties**.
3. On the **ws2019-08b-rsvault | Properties** blade, select the **Update** link under the **Backup Configuration** label.
4. On the **Backup Configuration** blade, set **Storage replication type** to **Locally-redundant**, select **Save** and close the **Backup Configuration** blade.

   Note: Storage replication type cannot be changed once you implement protection.

5. On the **ws2019-08b-rsvault | Properties** blade, select the **Update** link under the **Security Settings** label.
6. On the **Security Settings** blade, set **Soft Delete** to **Disable**, select **Save** and close the **Security Settings** blade.

16.4.1 Task 3: Install the Azure Recovery Services agent

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the Internet Explorer window displaying the Azure portal, on the **ws2019-08b-rsvault** Recovery Services vault blade, in the vertical menu, in the **Getting started** section, select **Backup**.
2. On the **ws2019-08b-rsvault |Backup** blade, specify the following settings:

   Table 15: Backup settings

Settings	Value
Where is your workload running?	On-premises
What do you want to backup?	Files and folders

   Note: Even though the virtual machine you are using in this task is running in Azure, you can leverage it to evaluate the backup capabilities applicable to any on-premises computer running Windows Server operating system.
3. On the **ws2019-08b-rsvault |Backup** blade, select **Prepare infrastructure**.
4. On the **Prepare infrastructure** blade, select the **Download Agent for Windows Server or Windows Client** link.
5. When prompted, at the bottom of Internet Explorer window, select **Run** to start installation of **MARSAgentInstaller.exe**. This will start the **Microsoft Azure Recovery Services Agent Setup Wizard**.
6. On the **Installation Settings** page of the **Microsoft Azure Recovery Services Agent Upgrade Wizard**, accept the default settings and select **Next**.
7. On the **Proxy Configuration** page of the **Microsoft Azure Recovery Services Agent Upgrade Wizard**, accept the default settings, and then select **Next**.
8. On the **Microsoft Update Opt-in** page of the **Microsoft Azure Recovery Services Agent Upgrade Wizard**, select **I do not want to use Windows Update**, and select **Next**.
9. On the **Installation** page of the **Microsoft Azure Recovery Services Agent Upgrade Wizard**, select **Install**.
10. After the installation completes, on the **Installation** page of the **Microsoft Azure Recovery Services Agent Upgrade Wizard**, select **Proceed to Registration**. This will launch the **Register Server Wizard**.
11. Switch to the Internet Explorer window displaying the Azure portal, on the **Prepare infrastructure** blade, select the checkbox **Already downloaded or using the latest Recovery Server Agent**, and select **Download**.
12. When prompted, whether to open or save the vault credentials file, select **Save**. This will save the vault credentials file to the local Downloads folder.
13. Switch back to the **Register Server Wizard** window and, on the **Vault Identification** page, select **Browse**.
14. In the **Select Vault Credentials** dialog box, browse to the **Downloads** folder, in the **Select Vault Credentials** dialog box, navigate to the **Downloads** folder, select the vault credentials file you downloaded, and select **Open**.
15. On the **Encryption Setting** page of the **Register Server Wizard**, select **Generate Passphrase**.
16. On the **Encryption Setting** page of the **Register Server Wizard**, select the **Browse** button next to the **Enter a location to save the passphrase** drop-down list.

17. In the **Browse For Folder** dialog box, expand **This PC** node, select the **Documents** subfolder and select **OK**.
18. Select **Finish**, review the **Microsoft Azure Backup** warning and select **Yes**, and wait for the registration to complete.

    Note: In a production environment, you should store the passphrase file in a secure location other than the server being backed up.

19. On the **Server Registration** page of the **Register Server Wizard**, review the warning regarding the location of the passphrase file, ensure that the **Launch Microsoft Azure Recovery Services Agent** checkbox is selected and select **Close**. This will automatically open the **Microsoft Azure Backup** console.

16.4.2 Task 4: Schedule Azure Backup

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, in the **Microsoft Azure Backup** console, in the **Actions** pane, select **Schedule Backup**.
2. In the **Schedule Backup Wizard**, on the **Getting started** page, select **Next**.
3. On the **Select Items to Backup** page, select **Add Items**.
4. In the **Select Items** dialog box, navigate to the **C:\Windows\System32\drivers\etc** folder, select **hosts**, and then select **OK**:
5. On the **Select Items to Backup** page, select **Next**.
6. On the **Specify Backup Schedule** page, ensure that the **Day** option is selected, in the first drop-down list box below the **At following times (Maximum allowed is three times a day)** box, select **4:30 AM**, and then select **Next**.
7. On the **Select Retention Policy** page, accept the defaults, and then select **Next**.
8. On the **Choose Initial Backup type** page, accept the defaults, and then select **Next**.
9. On the **Confirmation** page, select **Finish**. When the backup schedule is created, select **Close**.
10. In the **Microsoft Azure Backup** console, in the Actions pane, select **Back Up Now**.

    Note: The option to run backup on demand becomes available once you create a scheduled backup.

11. In the Back Up Now Wizard, on the **Select Backup Item** page, ensure that the **Files and Folders** option is selected and select **Next**.
12. On the **Retain Backup Till** page, accept the default setting and select **Next**.
13. On the **Confirmation** page, select **Back Up**.
14. When the backup is complete, select **Close**.
15. Switch to the Internet Explorer window displaying the Azure portal, navigate back to the **ws2019-08b-rsvault** Recovery Services vault blade and select **Backup items**.
16. On the **ws2019-08b-rsvault | Backup items** blade, select the **Azure Backup Agent** entry.
17. On the **Backup Items (Azure Backup Agent)** blade, verify that there is an entry referencing the **C:** drive of **ws2019-08-vm1.**.

16.4.2.1 Task 5: Perform file recovery by using Azure Recovery Services agent

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, open File Explorer, navigate to the **C:\Windows\System32\drivers\etc** folder and delete the **hosts** file.
2. Switch to the Microsoft Azure Backup window and select **Recover data**. This will start **Recover Data Wizard**.
3. On the **Getting Started** page of **Recover Data Wizard**, ensue that **This server (ws2019-08-vm1.)** option is selected and select **Next**.

4. On the **Select Recovery Mode** page, ensure that **Individual files and folders** option is selected, and select **Next**.
5. On the **Select Volume and Date** page, in the **Select the volume** drop down list, select **C:**, accept the default selection of the available backup, and select **Mount**.

   Note: Wait for the mount operation to complete. This might take about 2 minutes.
6. On the **Browse And Recover Files** page, note the drive letter of the recovery volume, select **Browse**, and review the tip regarding the use of **Robocopy**.
7. Select **Start**, expand the **Windows System** folder, and select **Command Prompt**.
8. From the **Administrator: Command Prompt** window, run the following to copy the restore the **hosts** file to the original location (replace `[recovery_volume]` with the drive letter of the recovery volume you identified earlier):

   ```
   robocopy [recovery_volume]:\Windows\System32\drivers\etc C:\Windows\system32\drivers\etc hosts /r:
   ```
9. From the **Administrator: Command Prompt** window, run the following to verify that the file has been restored:

   ```
   dir C:\Windows\system32\drivers\etc\hosts
   ```
10. Switch back to the **Recover Data Wizard** and, on the **Browse and Recover Files**, select **Unmount** and, when prompted to confirm, select **Yes**.

16.5 Exercise 5: Deprovisioning the Azure lab environment

16.5.1 Task 1: Remove the protected items

1. Within the Remote Desktop session to **ws2019-08-hvm0**, in the Virtual Machine Connection window to **ws2019-08-vm1**, switch to the Internet Explorer window displaying the **Backup Items (Azure Backup Agent)** blade of the Azure portal and select the entry referencing the **C:** drive of **ws2019-08-vm1.**.
2. On the **C:\ on ws2019-08-vm1.** blade, select the **ws2019-08-vm1.** link.
3. On the **ws2019-08-vm1.** blade, select **Delete**.
4. On the **Delete** blade, specify the following information, select the checkbox **There is backup data of 1 backup items associated with this server. I understand that clicking "Confirm" will permanently delete all cloud backup data. This action cannot be undone. An alert may be sent to the administrators of this subscription notifying them of this deletion**, and select **Delete**:

   Table 16: Backup item delete settings

Settings	Value
TYPE THE SERVER NAME	ws2019-08-vm1.
Reason	Decommissioned
Comments	Decommissioned
5. Close the Virtual Machine Connection window to **ws2019-08-vm1**, in the Remote Desktop session to **ws2019-08-hvm0**, in the Internet Explorer displaying the Azure portal, navigate to the **ws2019-08a-rsvault | Replicated items** blade, and select the **ws2019-08-vm1** entry.
6. On the **ws2019-08-vm1** replicated items blade, select the ellipsis in the toolbar and, in the drop-down menu, select **Disable replication**.
7. On the **Disable replication** blade, ensure that the **Disable replication and remove (Recommended)** entry appears in the **Remove replicated items** drop-down list, select **I don't want to provide feedback** checkbox, and select **OK**.

16.5.2 Task 2: Delete the lab resource groups

1. On **SEA-CL1**, close the Remote Desktop session to **ws2019-08-hvm0**, switch to the Microsoft Edge window displaying the Azure portal.

2. In the Azure portal, open the **Azure Cloud Shell** pane by selecting the Cloud Shell button in the Azure portal.
3. If prompted to select either **Bash** or **PowerShell**, and then select **PowerShell**.

   Note: If this is the first time you're starting **Cloud Shell** and you're presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and then select **Create storage**.
4. From the Cloud Shell blade, run the following command to delete all resource groups created throughout this lab:

   ```
   Get-AzResourceGroup -Name 'ws2019-08-*' | Remove-AzResourceGroup -Force -AsJob
   ```

   Note: The command executes asynchronously (as determined by the *-AsJob* parameter), so while you will be able to run another PowerShell command immediately after within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.